# Λύσεις ασκήσεων στην υπολογιστική θεωρία αριθμών

**Ευάγγελος Γκούμας**

**email:vaggoumas@gmail.com**

1) find all the primes of the form $\frac{n(n+1)}{2}$, $n \in \mathbb{N}$

<u>Solution</u>

for <u>$n=1$</u> $\frac{1(1+1)}{2} = 1$ not prime

for $n=2$ $\frac{2(2+1)}{2} = 3$ prime

for $n>2$ $\rightarrow$ if $2/n$ then $\frac{n}{2} = k$ so, the number has the form $k(n+1)$ which is not prime

if $2 \nmid n \Rightarrow 2/n+1$, Hence, $\frac{n+1}{2} = l$ so the number has the form $ln$ <u>not prime.</u>

## Άσκηση 2

(α) Να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής $4k+3$

**Λύση**

Για την δική μου ευκολία θέτω $k=n$

δηλαδή λύνω την "νέα" $4n+3$

Θα χρησιμοποιώσω την μαθηματική επαγωγή

υποθέτουμε ότι έχουμε πεπερασμένους πρώτους $p$ της μορφής $4n+3$

$p_1, p_2, \dots, p_k$

Έστω $n = 4p_1p_2\dots p_k - 1$

$m = 4n+3$ με $n = p_1p_2\cdot\ldots\cdot p_k - 1$

$$\boxed{\begin{aligned} m &= 4(p_1p_2\cdot\ldots\cdot p_k - 1) + 3 = \\ &= 4p_1p_2\dots p_k - 4 + 3 = \\ &\Rightarrow 1 = 4p_1p_2\dots p_k - m \end{aligned}}$$

Αφού $m$ περιττός ακέραιος έχουμε $p_1p_2\dots p_k$ είναι όλοι οι περιττοί πρώτοι, so $p_i$ είναι της μορφής $4n+3$ και $4n+1$ για κάποιο $n$.

Εάν $p_i$ έχει μορφή $4n+1$ τότε $m$ είναι $4n+1$ το οποίο είναι λάθος.

Ως εκ τούτου $m$ ~~έχει~~ διαιρείται από τουλάχιστον ένα πρώτο $p_i$

έστω ότι έχει τη μορφή $4n+3$ έχουμε $p_i / m \Rightarrow p_i = 4p_1p_2\cdot\ldots\cdot p_k$

$$\Downarrow$$

$$p_i / 4p_1p_2\dots p_k - m$$

$$\Downarrow$$

$$p_i / 1 \quad (1 = 4p_1p_2\dots p_k - m)$$

Αδύνατο, άρα υπάρχουν άπειροι πρώτοι της μορφής $4n+3$

(β) Γιατί ερώτημα το λύνουμε με ίδιο τρόπο αλλά το πυρήνα μουμε καταλήξει.

3) if $P_1, P_2, \ldots,$ a sequence of prime numbers. Prove that:

a) $P_n \leq P_1 \cdot \ldots \cdot P_{n-1} + 1$

b) $P_n < 2^{2^{n-1}}$

<u>solution</u>

b) Using mathematical induction

for $\underline{n=1}$ $P_1 < 2^{2^{1-1}} = 2^{2^0} = 2$

$\underline{n=k}$

$$P_k < 2^{2^{k-1}}$$

$\underline{n=k+1}$

$$P_{k+1} < 2^{2^{k+\cancel{1}-\cancel{1}}} = 2^{2^k}$$

Using the a) inequality we have

$$P_{k+1} \leq P_1 P_2 \cdot \ldots \cdot P_{k+\cancel{1}-\cancel{1}} + 1 = P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k + 1$$

$$< 2^{2^0}\, 2^{2^1} \cdot 2^{2^2} \cdot \ldots 2^{2^{k-1}} + 1 =$$

$$= \prod_{i=1}^{k} 2^{2^{i-1}} + 1 = 2^{\sum_{i=1}^{k} 2^{i-1}} + 1 < 2^{2^k}$$

a) I want to prove $P_n \leq P_1 \cdot \ldots \cdot P_{n-1} + 1$ ☒

Let $N = P_1 P_2 \ldots P_{n-1} + 1$ (from Euclid theorem)

The N has at least one prime divisor (m) so, $m / N$, $m \leq N$

and can't be $m = P_1, P_2, \ldots, P_{n-2}$

$\Downarrow$

$m = P_i \quad 1 \leq i \leq n-2 \longrightarrow P_i / N$ and $P_i / P_1 P_2 \ldots P_{n-2}$

$\Rightarrow P_i / N - P_1 P_2 \cdot \ldots \cdot P_{n-2} = 1$

contradiction

$(P_i \times 1)$

So, $m \geq P_n$

$\Rightarrow P_n \leq m \leq P_1 P_2 \cdot \ldots \cdot P_{n-1} + 1$

Hence $\boxed{P_n \leq P_1 P_2 \ldots P_{n-1} + 1}$ ☒

4) Prove for $n \geq 0$, $30 / n^5 - n$

<u>solution</u>

$30 = 2 \cdot 3 \cdot 5 \Rightarrow n = 30 = 2 \cdot 3 \cdot 5 = P_3 \cdot P_2 \cdot P_1$

I'm using Fermat little theorem.

$$n^p \equiv n \bmod p$$

for $P_1 = 5$ $\quad 5 / n^5 - n$

and $n^5 - n = n(n^4 - 1) = (n^2 - 1)(n^2 + 1)n = (n^3 - n)(n^2 + 1)$

$P_2 = 3$ $\quad 3 / n^3 - n$

As 3 divides $n^3 - n \Rightarrow 3 / n^5 - n$

$P_3 = 2$ $\quad 2 / n^2 - n$

As 2 divides $n^2 - n \Rightarrow 2 / n^5 - n$

so, $\operatorname{lcm}(2, 3, 5) = 30 \; / \; n^5 - n$.

As <u>second</u> way of solution we can use mathematical induction.

5) Find the highest power of 3 that divide 100!

<u>Solution</u>

From the theory we know the highest integer $r$ such that $p^r / n!$
we can find $r$ from the type (mathematical) $r = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$

$n = 100!$ $\quad p = 3$

Hence, $r = \left\lfloor \frac{100!}{3} \right\rfloor + \left\lfloor \frac{100!}{9} \right\rfloor + \left\lfloor \frac{100!}{27} \right\rfloor + \left\lfloor \frac{100!}{81} \right\rfloor =$

$= 33 + 11 + 3 + 1 = 48$

6) Find the prime factorization of the numbers

(a) $3^{12}-1$ , (b) 235679 , (c) 756943

Solution

(b) The number 235679 is a prime number. Hence, I can't do factorization

(c) $756943 = 68813 \times 11 \times 1$

(a) $3^{12}-1 = 531440 = 2^4 \times 5 \times 7 \times 13 \times 73$

7) Prove that for natural $\tau(n)$ is odd if and only if $n$ is perfect square.

<u>Solution</u>

From the definition of $\tau(n) = (a_1+1)(a_2+1)(a_3+1)\cdots(a_k+1)$

if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

($\Rightarrow$) -

So from the problem 7 we know that $\tau(n)$ is odd from above definition

$T(n) = (a_1+1)(a_2+1)\cdots(a_k+1)$ $T(n)$ is odd and $a_i$ must be even.

$\Rightarrow n = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} = (p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k})^2$ $n$ is perfect square

($\Leftarrow$) we know that $n$ is perfect square

$n = (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})^2 = p_1^{2a_1} \cdot p_2^{2a_2} \cdots p_k^{2a_k}$

$T(n) = \underbrace{(2a_1+1)}_{\text{odd}} \cdot \underbrace{(2a_2+1)}_{\text{odd}} \cdots \underbrace{(2a_k+1)}_{\text{odd}}$

So, $T(n)$ is odd

$\blacksquare$

8)

Let $n$ integer $n > 1$ and $p_1, p_2, \ldots, p_k$ primes and divisors of $n$

<u>Prove</u> $1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

<u>Solution</u>

from number theory we have Euler function $\varphi(n)$ which is a multiplicative function.

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) =$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}$$

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$1 > \frac{n}{\sigma(n)} > \frac{\varphi(n)}{n}$$

$$\sigma(n) = n \prod_{p_i / n} \frac{1 - p_i^{-a-1}}{1 - p^{-1}}$$

$$\frac{\sigma(n)\,\phi(n)}{n^2} = \prod_{p_i / n} \left(1 - p_i^{-a-1}\right) < 1$$

So, $\frac{\sigma(n)\,\phi(n)}{n^2} < 1 \Leftrightarrow \frac{\sigma(n)}{n} < \frac{n}{\phi(n)} \Leftrightarrow$

$$\boxed{1 > \frac{n}{\sigma(n)} > \frac{\phi(n)}{n} = \prod_{p_i=1}^{k} \left(1 - \frac{1}{p_i}\right)}$$

9)

a) For $n \geq 3$ prove $\sum_{k=1}^{n} \mu(k!) = 1$

<u>Solution</u>

From theory we know $\mu(1) = 1$

$$\mu(n) = \begin{cases} (-1)^k, & \text{if } a_1 = a_2 = \dots = a_k = 1 \\ 0, & \text{else} \end{cases}$$

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

from the table we have

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 . . . |
|---|---|---|---|---|---|---|---|
| $\mu(n)$ | 1 | -1 | -1 | 0 | -1 | 1 | -1 . . . |

for our case we want to prove:

$$\sum_{k=1}^{n} \mu(k!) = 1$$

So, $\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) + \dots + \mu(n!) =$

$= \mu(1) + \mu(2) + \mu(6) + \dots + \mu(n!) =$

$= 1 + (-1) + 1 + \dots = 1$ ∎

b) For any positive integer $n$ prove $\mu(n) \cdot \mu(n+1) \mu(n+2) \mu(n+3) = 0$

<u>Solution</u>

Given four any consecutive integers $n, n+1, n+2, n+3$ one of them will be divisible by 4. If this integer is $K$, then $\mu(K) = 0$

∎

10)

a) Prove that Fermat number $F_4$ is prime

<u>Solution</u>

From the theory Fermat number has the form $F_n = 2^{2^n} + 1$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65.537$$

So, $F_4 = 65.537$ is prime number.

b) Let $n$ odd perfect integer and $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then $p_1 = 1 + 4b$, $a_1 = 1 + 4c$ when $b, c$ natural numbers $a_2, \dots, a_k$ <u>even</u>

<u>Solution</u>

$$\sigma(n) = \prod_k (1 + p_1 + p_1^2 + \dots + p_1^k)$$

$$1 + p_1 + \dots + p^k = \begin{cases} a + 1 \bmod 4 & p_1 \equiv \bmod 4 \\ 0 \bmod 4 & 2 \nmid a, p_1 \equiv -1 \bmod 4 \\ 1 \bmod 4 & 2 \mid a, p \equiv -1 \bmod 4 \end{cases}$$

$2n$ is not ~~multiple~~ multiple of 4 so $p \equiv 1 \bmod 4$

$ap \equiv 1 \bmod 4$.

1) Έστω $A, B, \Gamma \in \mathcal{B}(E)$ τότε για το $\cap$ ισχύει

Τότε $(A \cap B) \cap \Gamma = A \cap (B \cap \Gamma)$ , $A \cap E = E \cap A = A$ , ($E$ ουδέτερο)

Ένωση $(A \cup B) \cup \Gamma = A \cup (B \cup \Gamma)$ στην ένωση το ουδέτερο στοιχείο είναι το κενό $\phi$

$A \cup \phi = A \ \forall A \in \mathcal{B}(E)$

Άρα μονοειδή

$f: A \longrightarrow A^c$ $e_\cap = E$ , $e_\cup = \phi$ τα ουδέτερα στοιχεία του $(\mathcal{B}(E), \cap)$ και $(\mathcal{B}(E), \cup)$ αντίστοιχα

$$f(e_\cap) = f(E) = E^c = \phi = e_\cup \rightarrow f(e_\cap) = f(e_\cup)$$

$$f(A \cap B) = (A \cap B)^c = A^c \cup B^c = f(A) \cup f(B)$$

Άρα $f$ ομομορφισμός μονοειδών

Αρκεί νδο ισομορφισμός

1-1 $f(A) = f(B) \Leftrightarrow A^c = B^c \Leftrightarrow A = B$

$\forall A \in (\mathcal{B}(E), \cup)$ $A^c \in (\mathcal{B}(E), \cap)$ με $f(A^c) = A$

Άρα ισομορφισμός μονοειδών

2) a) Έστω $S$ υποομάδα του $G$ Τότε $e_G \in S$ άρα $f(e_G) = e_H \in f(S)$

Έστω $s_1, s_2 \in S$ τέτ. $s_1 * s_2 \in S \rightarrow f(s_1 * s_2) \in f(S)$

$\Rightarrow f(s_1) * f(s_2) \in f(S)$

Ισοδύν. εάν $h_1, h_2 \in f(S) \Rightarrow h_1 = f(s_1),\ h_2 = f(s_2)$ $h_1 * h_2 \in f(S)$

Άρα $f(S)$ υποομάδα του $f(S)$

b) Έστω $T$ υποομάδα του $H$ Τότε $e_H \in T \Rightarrow f^{-1}(e_H) = e_S \in f^{-1}(T)$

Αν $t_1, t_2 \in f^{-1}(T) \Rightarrow t_1 = f^{-1}(h_1),\ t_2 = f^{-1}(h_2)\ \forall h_1, h_2 \in H$

Άρα $t_1 * t_2 = f^{-1}(h_1) * f^{-1}(h_2) \Rightarrow f^{-1}(h_1 * h_2) \in f^{-1}(T)$

Άρα $f^{-1}(T)$ υποομάδα του $S$

3) Έστω $(H_i)_{i\in I}$ μια ~~μια~~ οικογένεια υποομάδων μιας ομάδας $G$.
Ν.δ.ο η τομή $\bigcap_{i\in I} H_i$ είναι υποομάδα της $G$.

<u>Λύση</u>

Από την θεωρία ξέρουμε ότι η $H \leq G$ (υποομάδα) εάν ισχύουν τα εξής: i) $\forall\, h_1, h_2 \in H$ τότε $h_1 h_2 \in H$

ii) $\forall\, h \in H$ το $h^{-1} \in H$

Έστω $H$ η παραπάνω τομή και $h_1, h_2 \in H$ άρα $h_1, h_2 \in H_i$ για κάθε $i \in I$ και επειδή $H_i \leq G$ είναι $h_1 h_2 \in H_i$ $\forall\, i \in I$, συνεπώς $h_1 h_2 \in H$. Επίσης εάν $h \in H_i$ $\forall\, i \in I$ τότε $h^{-1} \in H$.

5)

Έστω $f$ αριθμητική συνάρτηση. Ορίζουμε δεύτερη αριθμητική συνάρτηση $F$ από τη σχέση $F(n) = \sum_{d/n} f(d)$ για κάθε ακέραιο. Να δείξετε η $f$ είναι πολλαπλασιαστική εάν και μόνον εάν η $F$ είναι πολλαπλασιαστική

Λύση

Σχόλια Για αυτό τον άσκηση έχει εξαιρετικά και θέλει γνώση αναλυτικής θεωρίας αριθμών. Θα αξιοποιήσουν τον συνδυασμό Inverse Möbius

~~Έστω $f$ και $g$ δύο αριθμητικές συναρτήσεις ορίζουμε κατά Dirichlet Dirichlet γινόμενο (συνέλιξη Dirichlet) μιας αριθμητικής συνάρτησης. Η οποία ορίζεται ως εξής~~

$$\cancel{h(n) = \sum_{d/n} f(d) g\left(\frac{n}{d}\right)}$$

$(\Longrightarrow)$

Εστω $f(n) = \sum_{d/n} g(d) \Longrightarrow g(n) = \sum_{d/n} f(d)\mu\left(\frac{n}{d}\right)$

Τύπος αντιστροφής Möbius

$$F(n) = \sum_{d/n} f(d) \xrightarrow[\text{Möbius}]{} f(n) = \sum_{d/n} F(d)\mu\left(\frac{n}{d}\right)$$

Inverse

Τώρα θέλουμε νέα $f(n) = \sum_{d/n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d/n} \mu(d) F\left(\frac{n}{d}\right)$

Εστω $n = n_1 n_2$

$$f(n_1 n_2) = \sum_{d/n_1 n_2} F(d)\mu\left(\frac{n_1 n_2}{d}\right) = \sum_{d/n_1 n_2} \mu(d) F\left(\frac{n_1 n_2}{d}\right) =$$

$$= \sum_{d/n_1 n_2} \mu(d) F\left(\frac{n_1}{d}\right) \cdot F\left(\frac{n_2}{d}\right) = \sum_{d/n_1} \mu(d) F\left(\frac{n_1}{d}\right) \cdot \sum_{d/n_2} \mu(d) F\left(\frac{n_2}{d}\right) =$$

$= f(n_1) \cdot f(n_2)$ Άρα πολλαπλασιαστική

$(\Leftarrow)$

Η $f$ είναι πολλαπλασιαστική άρα

έστω $n = n_1 \cdot n_2$

$(d_1, d_2) = 1$

$$F(n) = F(n_1 n_2) = \sum_{d / n_1 n_2} f(d_1 d_2) =$$

$$= \cancel{\sum_{d_1/n_1} f(d_1 d_2) \sum_{d_2/n_2} f} = \sum_{d_1/n_1} f(d_1) \sum_{d_2/n_2} f(d_2) =$$

$$= F(n_1) \cdot F(n_2)$$

6) $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \tau(d)$

Λύση

Ορίζω $F(n) = \sum_{d|n} \sigma(d)$ , $G(n) = n \sum_{d|n} \frac{\tau(d)}{d}$

Η σ πολλαπλασιαστική $\Rightarrow$ F πολλαπλασιαστική

τ -//- $g(n) = 1/n$ πολ/κη $\Rightarrow \frac{\tau(n)}{n}$ πολλ/κή

$\Rightarrow \sum_{d|n} \frac{\tau(d)}{d}$ πολ/κη $\Rightarrow$ G πολλ/κη

$F(1) = G(1) = 1$

• Έστω $n = p^a$ $\quad G(p^a) = F(p^a)$ (*)

$$F(p^a) = \sigma(1) + \sigma(p) + \dots + \sigma(p^a) = 1 + \frac{p-1}{p-1} + \dots + \frac{p^{a+1}-1}{p-1} =$$

$$= \frac{p + p^2 + \dots + p^{a+1} - (a+1)}{p-1}$$

$$G(p^a) = p^a\left(1 + \frac{2}{p} + \dots + \frac{a+1}{p^a}\right) = p^a + 2p^{a-1} + \dots + (a+1)$$

$$(*) \Rightarrow p + p^2 + \dots + p^{a+1} - (a+1) = (p-1)(p^a + 2p^{a-1} + \dots + (a+1))$$

$$\Rightarrow p + p^2 + \dots + p^{a+1} - (a+1) = p^{a+1} + 2p^a + \dots + p(a+1) - p^a - 2p^{a-1} - (a+1)$$

$\Rightarrow$ η (*) ισχύει

$$\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} d\,\tau(d)$$

<u>Làm</u>

$$\sigma(d) = \sum_{d_1|d} d$$

$$\tau(d) = \sum_{d_1|d} 1$$

$$\sum_{d|n} \frac{n}{d}\sigma(d) = \sum_{d|n} \frac{n}{d} \sum_{d_1|d} d_1 = \sum_{d|n} \sum_{d_1|d} \frac{n}{d/d_1} = \sum_{\substack{n=de \\ d=d_1d_2}} \frac{n}{d/d_1} = \sum_{n=d_1d_2e} \frac{n}{d_2} =$$

$$= \sum_{n=d_1d_2} d_1 e = \sum_{d|n} d\,\tau(d)$$

7) Να προσδιοριστούν οι ενδομορφισμοί και αυτομορφισμοί $(\mathbb{Z},+)$ και $(\mathbb{Q},+)$

Λύση

Έστω $f:\mathbb{Z}\to\mathbb{Z}$ ομομορφισμός $f(n+m)=f(n)+f(m)$

$\forall n,m\in\mathbb{Z}$ Άρα $f(n)=nf(1)$

Το $f(1)=1 \Rightarrow f(n)=n\ \forall n\in\mathbb{N} \Rightarrow f\equiv id$

Εάν $f(1)=-1$, $f(n)=-n\ \forall n\in\mathbb{Z}$

Εάν $f(1)=k$. Αφού $1\in\mathbb{Z}$ και $f$ επί υπάρχει $l\in\mathbb{Z}$

τ.ω $f(l)=1$. Άρα $f(1)=k=1+1+\dots+1=f(l)+\dots+f(l)$

$\Rightarrow f(1)=f(kl)$ Αφού $f$ 1-1 $\Rightarrow 1=kl$, $k\neq\pm1$

Άτοπο Άρα υπάρχουν μόνο δύο αυτομορφισμοί του $\mathbb{Z}$

$\mathbb{Z}\to\mathbb{Z}$ $\quad$ $\mathbb{Z}\to\mathbb{Z}$

$1\mapsto 1$ $\quad$ $1\mapsto -1$

Εάν $f:\mathbb{Z}\to\mathbb{Z}$ δεν είναι 1-1 και επί αλλά ομομορφισμός τότε $f(1)=k\in\mathbb{Z}$

και $f:\mathbb{Z}\to\mathbb{Z}$, $n\mapsto kn$ ενδομορφισμοί

Έστω $f:\mathbb{Q}\to\mathbb{Q}$ ομομορφισμός για $x,y\in\mathbb{Q}$ $f(x+y)=f(x)+f(y)$

Άρα $f\left(\frac{m}{n}\right)=m\,f\left(\frac{1}{n}\right)$

Αν $f(1)=1 \Rightarrow f\equiv id$ Αν $f(1)=-1 \Rightarrow f\left(\frac{m}{n}\right)=-\frac{m}{n}$

Αν $f(1)=k\neq\pm1$ $f\left(\frac{m}{n}\right)=k\frac{m}{n}$. $\forall k\neq0$

$f\left(\frac{m_1}{n_1}\right)=f\left(\frac{m_2}{n_2}\right) \Leftrightarrow$

$k\frac{m_1}{n_1}=k\frac{m_2}{n_2} \Leftrightarrow$

$\frac{m_1}{n_1}=\frac{m_2}{n_2} \to f$ 1-1

Αν $x\in\mathbb{Q} \to x=\frac{r}{d}$ $\exists y\in\mathbb{Q}$ τ.ω $f(y)=\frac{r}{d}$

Με $y=\frac{r}{d} \Rightarrow f$ επί

8) Να προσδιοριστούν οι ενδομορφισμοί και αυτομορφισμοί μιας κυκλικής ομάδας

Solution

Let $G$ a cyclic group

Automorphism

i) if $G$ is infinite, $Aut\ G$ consits of the identity automorphism and the automorphism $g \longrightarrow g^{-1}$. So $Aut\ G$ is a cyclic of order 2

ii) if $G$ has finite order $n$, then $Aut\ G$ consists of all automorphism $(|G| = n)$

$\alpha_k : g \longrightarrow g^k$, $1 \leq k \leq n$ and $(k,n) = 1$, moreover the mapping $k + nZ \longrightarrow \alpha_k$ is an isomorphism from $Z_n^*$ to $Aut\ G$. In particular $Aut\ G$ is abelian and has order $\varphi(n)$ ($\varphi(n)$ Euler function)

Endomorphism

9) Έστω $S$ μη-κενό υποσύνολο της ομάδας $G$. Τότε $\langle S \rangle = \{x_1^{a_1} \dots x_n^{a_n} : n \geq 1\}$
$(S \subseteq G)$

Θα δείξουμε ότι $\langle S \rangle$ είναι υποομάδα της $G$ που περιέχει το $S$ και είναι υποομάδα παραγόμενη από το $S$

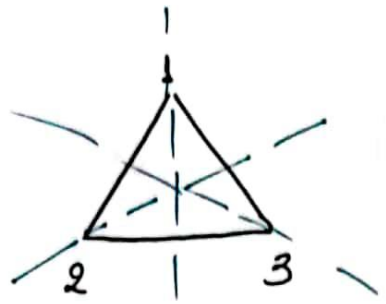
Έστω $z = x_1^{a_1} \cdot \dots \cdot x_m^{a_m}$ και $w = y_1^{b_1} \cdot y_2^{b_2} \cdot \dots \cdot y_r^{b_r}$ είναι δύο στοιχεία του $\langle S \rangle$

$zw^{-1} = x_1^{a_1} \cdot \dots x_m^{a_m} (y_1^{b_1} \cdot \dots \cdot y_r^{b_r})^{-1} = x_1^{a_1} \cdot \dots \cdot x_m^{a_m} y_r^{-b_r} \cdot \dots \cdot y_1^{-b_1}$

και επομένως $zw^{-1} \in H$ Η $\langle S \rangle$ υποομάδα δηλαδή $S \subseteq \langle S \rangle$

Αν $S = \{a_1, \dots, a_k\}$ τότε $\langle a_1, \dots, a_k \rangle$.

10)




$\rho_i$: οι στροφές

$\mu_i$: οι ανακλάσεις ως προς τις μεσοκαθέτους

$$id = \rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

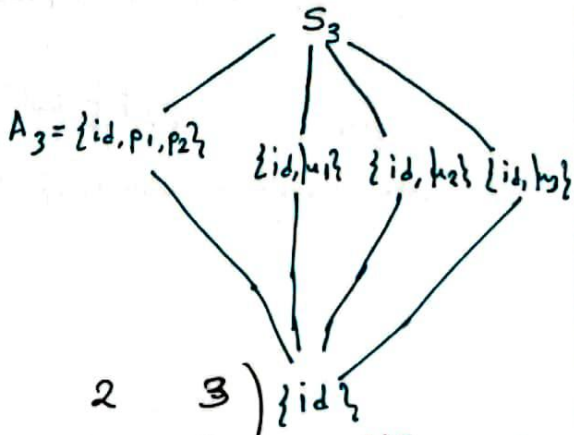
$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Με βάση την θεωρία έχουμε ότι μια ομάδα λέγεται abelian εαν για κάθε $a, b \in G$ ισχύει ότι $ab = ba$.

Εκμεταλευόμενοι το παραπάνω έχουμε ότι έστω $\sigma$ (με $\sigma$ συμβολίζουν τη μετάθεση μου (permutation)) και $\rho$ όπου $\sigma, \rho \in \underline{S_3}$

Έστω:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$




υποομάδες της $S_3$

$$\sigma\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Άρα $\sigma\rho \neq \rho\sigma$ άρα αντιμεταθετικός

11)

$$(a_1\ a_2 \dots a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{k+1} & \dots & a_n \\ a_2 & a_3 & \dots & & a_{k+1} & \dots & a_n \end{pmatrix}$$

Νδο κάθε μετάθεση αναλύεται κατά μοναδικό τρόπο σε γινόμενο ξένων κύκλων ξένους ανά δύο

<u>Απόδειξη</u>

Έστω σ μια μετάθεση βαθμού n. Παίρνουμε ένα στοιχείο $i_1 \in \{1, 2, \dots, n\}$ και ξεκινάμε έναν κύκλο $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, κ.λ.π. Υποθέτω ότι τα $i_1, i_2, \dots, i_n$ είναι διαφορετικά και το $\sigma(i_k) \in \{i_1, i_2, \dots, i_n\}$. Εάν $\sigma(i_k) = i_1$ έχουμε έναν κύκλο και δεν υπάρχει άλλος.

Εάν $\sigma(i_k) = i_l$ $\quad 2 \le l \le k$ τότε $\sigma(i_{l-1}) = i_l = \sigma(i_k)$ όπου αυτό αντιβαίνει στον ~~ορισμό~~ ορισμό της μετάθεσης που ξέρουμε ότι είναι 1-1 αντικατάσταση.

Αλλιώς $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Παρατηρούμε ότι $\sigma = (i_1 i_2 i_3 \dots i_k)\sigma'$ όπου $\sigma'$ δεν μας μετακινεί κάποιο στοιχείο του συνόλου $\{i_1, i_2, \dots, i_k\}$ και δρα ~~σο~~ σ ως συμπληρωματικό στο σύνολο. Αυτό έχει σαν αποτέλεσμα να δημιουργούμε ξένους κύκλους μεταθέσεων.

12) $\varphi : R \longrightarrow R' \quad \forall r_1, r_2 \in R$ $\quad \varphi(r_1) = r_1'$, $\varphi(r_2) = r_2'$

a) $\phi : R' \longrightarrow R'' \quad \forall r_1', r_2' \in R'$ $\quad \phi(r_1') = r_1''$ $\phi(r_2') = r_2''$

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[rr, bend right, "\phi \circ \varphi"'] & R' \arrow[r, "\phi"] & R'' \end{tikzcd}$$

$$\phi \circ \varphi(r_1 + r_2) = \phi(r_1' + r_2') = r_1'' + r_2'' = \phi(\varphi(r_1)) + \phi(\varphi(r_2))$$

$$\phi \circ \varphi(r_1 \cdot r_2) = \phi(r_1' \cdot r_2') = r_1'' \cdot r_2'' = \phi(\varphi(r_1)) \cdot \phi(\varphi(r_2))$$

b)

$$\begin{tikzcd} R \arrow[r, bend left, "\varphi"] & R' \arrow[l, bend left, "\varphi^{-1}"] \end{tikzcd}$$

$\varphi(r) = r' \quad \forall \underline{r \in R}$

$\varphi^{-1}(r') = r \quad \forall r' \in R'$

$\cancel{\varphi^{-1}(r_1 + r_2) = \varphi^{-1}(r_1) + \varphi^{-1}(r_2)}$

$\cancel{\varphi^{-1}(r_1 \cdot r_2) = \varphi^{-1}(r_1') \cdot \varphi^{-1}(r_2')}$

$\varphi^{-1}(r_1' + r_2') = r_1 + r_2 =$
$= \varphi^{-1}(r_1') + \varphi^{-1}(r_2')$

$\varphi^{-1}(r_1' \cdot r_2') = r_1 \cdot r_2 =$
$= \varphi^{-1}(r_1') \cdot \varphi^{-1}(r_2')$

c) let $a, b \in A$ $f(a)$ and $f(b)$ are in $f$ because $f$ is homorphism so $f(a+b)$ is also in $f(A)$. Hence, $f(a+(-b)) \in f(A)$ so $A + (-b) \in A$

$a \cdot b \in f(A)$ $a, b \in A$ $f(a)$ and $f(b) \in f$ $f$ is homomorphism so $f(ab)$ is also in $f(A)$ so $f(A)$ subring of $B$

13) $f: \mathbb{Z} \to \mathbb{Z}$, $f(1) = 1$

$f(a+b) = f(a) + f(b)$ using for $n \geq 1$ we get

$$f(n) = f(1+1+\dots+1) = f(1) + f(1) + \dots + f(1) = n f(1)$$

and $f(-n) = f((-1)+\dots+(-1)) = n f(-1)$

$$f(-1) + f(1) = f(-1+1) = f(0) = 0$$

And from theory we have $f(-1) = -f(1)$. Hence $f$ is completely determined by $f(1)$ via $f(k) = k f(1)$ $\forall k \in \mathbb{Z}$

Also, $f(1) = f(1^2) = f(1)^2$ which means in $\mathbb{Z}$ $f(1) = 1$ or $f(1) = 0$ if $f$ ought to be unital, so $f \equiv id$.

16)

Να δειχθεί ότι $P(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$ δεν έχει ρίζα με πολλαπλότητα $> 1$ κάποια στο $\mathbb{C}$

<u>Λύση</u>

Έστω $x=0$ $P(0) = 1 + 0 + 0 + \dots + 0 = 1$, άρα το 0 δεν είναι ρίζα. Τότε $P(x) = P'(x) + \frac{x^n}{n!}$ έτσι $P(x) = 0$, έχουμε $P'(x) \neq 0$ Άρα είναι ρίζα απλή (simple root) στο $\mathbb{C}$

1β)

$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$

Με αυτή μέθοδο αντικατάστασης όπου για όπου $x = q(x)$

$P(q(x)) =$

$= a_n (q(x))^n + a_{n-1} \cdot (q(x))^{n-1} + \dots + a_1 (q(x)) + a_0$

```
for i = 0,1,n
    for j = 0,1,m
        q(x) = Σ_{j=0}^{m} b_j x^j
    end for
    P(q(x)) = Σ_{i=0}^{n} a_i (q(x))^i
end for
```

L9)

$P(x) = 2x^4 + 5x^2 - x + 10 \qquad Q(x) = x^3 + 5x + 1$

<u>Λύση</u>

$$2x^4 + 5x^2 - x + 10 = (x^3 + 5x + 1)(2x) + (-5x^2 - 3x + 10)$$

$$x^3 + 5x + 1 = (-5x^2 - 3x + 10)\left(-\frac{1}{5}x + \frac{3}{25}\right) + \left(\frac{184}{25}x - \frac{1}{5}\right)$$

$$-5x^2 - 3x + 10 = \left(\frac{184}{25}x - \frac{1}{5}\right)\left(-\frac{125}{184}x - \frac{14425}{33856}\right) + \left(\frac{335675}{33856}\right)$$

$$\frac{184}{25}x - \frac{1}{5} = \left(\frac{335675}{33856}\right)\left(\frac{6229504}{8391875}x - \frac{33856}{1678375}\right) + 0$$

$$\gcd\big(P(x), Q(x)\big) = 1$$

Με αντικατάσταση (Αντίστροφο Ευκλείδη)

$$D = 1 = \underbrace{\left(\frac{184}{13427}x^2 + \frac{5}{13427}x + \frac{1285}{13427}\right)}_{U(x)}\overbrace{\left(2x^4 + 5x^2 - x + 10\right)}^{P(x)}$$

$$+ \underbrace{\left(-\frac{368}{13427}x^3 - \frac{10}{13427}x^2 - \frac{1650}{13427}x + \frac{577}{13427}\right)}_{V(x)}\overbrace{\left(x^3 + 5x + 1\right)}^{Q(x)}$$

14) Làm

$$P(x+c) = c_0 + c_1 x + \dots + c_d x^d$$

$$P'(x+c) = c_1 + 2c_2 x + \dots + d c_d x^{d-1}$$

$$\vdots$$

$$P^{(d)}(x+c) = d(d-1)\cdot \dots \cdot 2\cdot 1\, c_d = d!\, c_d$$

Tại $x=0$

$$\begin{cases} c_0 = P(c) \\ c_1 = P'(c) \\ c_2 = \frac{1}{2!} P''(c) \\ \vdots \\ c_d = \frac{1}{d!} P^{(d)}(c) \end{cases}$$

$$\Rightarrow P(x+c) = P(c) + x P'(c) + \frac{1}{2} x^2 P''(c) + \dots + \frac{1}{d!} x^d P^d(c)$$

17)

$$\begin{array}{l|l} \cancel{x^m} - 1 & x^n - 1 \\ \hline -\cancel{x^m} + \frac{x^m}{x^n} & \frac{x^m}{x^n} \\ \hline \frac{x^m}{x^n} - 1 & \\ \quad \parallel & \\ x^n - 1 & \end{array}$$

$$x^m = x^{nq} \cdot x^r \Leftrightarrow$$

$$\frac{x^m}{x^n} = x^r$$

$$m = n \cdot q + r$$

Άρα $x^m - 1 = (x^n - 1)\left(\frac{x^n}{x^n}\right) + x^r - 1$

Άρα το $x^r - 1$ είναι το υπόλοιπο του $\underline{x^m - 1}$ στο $\underline{x^n - 1}$

1) Να υπολογιστεί το υπόλοιπο της διαίρεσης $12^{23} \cdot 19^{37}$ με το 8

Λύση

$12 \equiv 4 \mod 8 \Leftrightarrow$

$12^2 \equiv 16 \mod 8 \Leftrightarrow$

$12^2 \equiv 0 \mod 8 \Leftrightarrow$

$(12^2)^{10} \equiv 0^{10} \mod 8 \Leftrightarrow$

$12^{20} \equiv 0 \mod 8 \Leftrightarrow$

$12^{20} \cdot 12^3 \equiv 0 \mod 8$ (1)

Άρα χωρίς να κάνουμε και το υπόλοιπο $19^{37} \equiv ? \mod 8$

και από την (1) εξάγουμε ότι έχουμε υπόλοιπο 0 (μηδέν)

$$\boxed{12^{23} \cdot 19^{37} \equiv 0 \mod 8}$$

2) Αν $a, b, n, k \in \mathbb{Z}$ με $k \neq 0$ και $d = \gcd(n, k)$

νδο εαν $ka \equiv kb \pmod{n} \Leftrightarrow a \equiv b \left(\bmod \frac{n}{d}\right)$

<u>Λύση</u>

($\Rightarrow$) Από την $ka \equiv kb \pmod{n}$ έπεται ότι $n / k(a-b)$ οπότε $\frac{n}{d} \Big| \frac{k}{d}(a-b)$

Αλλά $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$. Επομένως $\frac{n}{d} \Big| (a-b) \Leftrightarrow$

$$a \equiv b \left(\bmod \frac{n}{d}\right)$$

($\Leftarrow$) $a \equiv b \left(\bmod \frac{n}{d}\right)$ για την απόδειξη κάνω ότι και επάνω με φορά από τα δεξιά προς τα αριστερά.

$$a \equiv b \left(\bmod \frac{n}{d}\right) \Rightarrow \frac{n}{d} \Big| (a-b) \Leftrightarrow n / (a-b)d$$

$$\Rightarrow n \mid (a-b)dk' \Rightarrow n / (a-b)k \Rightarrow n / (ka-kb) \Leftrightarrow$$

$$\underline{ka \equiv kb \pmod{n}}$$

3)

Αν $a$ και $b$ είναι ακέραιοι που δεν διαιρούνται από το 3, να δειχθεί ότι ο ακέραιος $a^2+b^2$ δεν είναι τέλειο τετράγωνο ακεραίου

<u>Λύση</u>

Έχουμε $a^2+b^2 \equiv 0$ ή $1$ ή $2 \bmod 3$

Εάν $a^2+b^2 \equiv 0 \bmod 3$, $a, b \not\equiv 0 \bmod 3$ και $a^2, b^2 \not\equiv 0 \bmod 3$

$a^2 \equiv 1 \bmod 3$, $b^2 \equiv 2 \bmod 3$

Άρα $a$ ρίζα της εξίσωσης $x^2 \equiv 1 \bmod 3$ και $b$ ρίζα της $x^2 \equiv 2 \bmod 3$

Άτοπο αφού $1 = \left(\frac{2}{3}\right) \equiv 2^{\frac{3-1}{2}} \bmod 3 \equiv 2 \bmod 3$ <u>άτοπο</u>

Έστω ότι $a^2+b^2 \equiv 1 \bmod 3 \Leftrightarrow$

$a^2 \equiv b^2 \equiv 2 \bmod 3$ που είναι <u>αδύνατο</u>

Ως εκτός $a^2+b^2 \equiv 2 \bmod 3 \Leftrightarrow$

$a^2 \equiv b^2 \equiv 1 \bmod 3$

Έχουμε ότι η λύση της $a^2+b^2 \equiv x^2 \bmod 3$ και αφού

$n^2 \equiv 1 \bmod 3$ έχουμε $\left(\frac{2}{3}\right) = 1$, <u>άτοπο</u>

4) Να δειχθεί ότι για κάθε ακέραιο $n$ ισχύει $2730 / n^{13} - n$

Λύση

Έχουμε τον αριθμό $2730$ ο οποίος αναλύεται σε γινόμενο πρώτων παραγόντων

$$2730 = 2 \times 3 \times 5 \times 7 \times 13$$

Από Euler - Fermat θεώρημα έχουμε:

$$n^{\varphi(p)} \equiv 1 \mod p \quad , \quad (n,p) = 1$$

- $\varphi(2) = 1$
- $\varphi(3) = 2$
- $\varphi(5) = 4$
- $\varphi(7) = 6$
- $\varphi(13) = 12$

$\Longrightarrow n^{\varphi(2)} = n \equiv 1 \mod 2 \Longrightarrow \underline{n^{13} \equiv n \mod 2}$ (1)

$\Longrightarrow n^{\varphi(3)} = n^2 \equiv 1 \mod 3 \Longrightarrow (n^2)^6 \cdot n \equiv n \mod 3 \Longrightarrow \underline{n^{13} \equiv n \mod 3}$ (2)

$\Longrightarrow n^{\varphi(5)} = n^4 \equiv 1 \mod 5 \Longrightarrow (n^4)^3 \cdot n \equiv 1^3 \cdot n \mod 5 \Longrightarrow \underline{n^{13} \equiv n \mod 5}$ (3)

$\Longrightarrow n^{\varphi(7)} = n^6 \equiv 1 \mod 7 \Longrightarrow (n^6)^2 \cdot n \equiv 1^2 \cdot n \mod 7 \Longrightarrow n^{13} \equiv n \mod 7$ (4)

$\Longrightarrow n^{\varphi(13)} = n^{12} \equiv 1 \mod 13 \Longrightarrow n^{12} \cdot n \equiv n \mod 13 \Longrightarrow n^{13} \equiv n \mod 13$ (5)

Οι (1), (2), (3), (4), (5) γράφονται:

$$\begin{cases} 2 / n^{13} - n \\ 3 / n^{13} - n \\ 5 / n^{13} - n \\ 7 / n^{13} - n \\ 13 / n^{13} - n \end{cases} \xRightarrow{\text{γινόμενο}} \underline{2 \times 3 \times 5 \times 7 \times 13 / n^{13} - n} \Longleftrightarrow \boxed{2730 / n^{13} - n}$$

$\blacksquare$

5) Να δειχθεί ότι ο αριθμός $\dfrac{7\cdot 1968^{1968} - 3\cdot 68^{78}}{10}$ είναι ακέραιος

Λύση

Αρκεί να δείξουμε ότι $A = 7\cdot 1968^{1968} - 3\cdot 68^{78}$

$10 \mid A$

$10 = 2\cdot 5$ και $(2,5)=1$ $*$

• $7\cdot 1968^{1968} - 3\cdot 68^{78} = 2k,\ k\in\mathbb{Z}$

$\Rightarrow 2 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$ (1)

Μικρό θεώρημα Fermat $\underline{a^{p-1} \equiv 1 \bmod p}$

$\Rightarrow 3^4 \equiv 1 \pmod 5$

$1968^{1968} \equiv 3^{1968} \equiv (3^4)^{492} \equiv 1 \bmod 5$

$68 \equiv 3 \bmod 5 \Rightarrow$

$68^{78} \equiv 9 \equiv 4 \bmod 5$

$\Rightarrow 7\cdot 1968^{1968} - 3\cdot 68^{78} \equiv 7 - 3\cdot 4 \equiv -5 \equiv 0 \bmod 5$

$\Rightarrow 5 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$ (2)

$A \overset{(1)}{\underset{(2)}{\Longrightarrow}} \underline{10 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}}$.

6) Α p περιττός πρώτος, να δειχθεί ότι η πολυωνυμική ισοτιμία $x^2+1 \equiv 0 \bmod p$ έχει λύση εαν και μόνο εαν $p \equiv 1 \pmod 4$

<u>Λύση</u>

Ο p είναι περιττός πρώτος αριθμός, έστω $k = \frac{(p-1)}{2}$

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot k \cdot (k-1) \cdot \ldots \cdot (p-2) \cdot (p-1)$$

Έχουμε $p-1 \equiv -1,\ p-2 \equiv -2, \ldots, k+1 \equiv p-k \equiv -k \pmod p$

Άρα με αντικατάσταση κάθε k παράγοντα από τον $p-i$ με $-i$ για $i = 1, \ldots, k$

Βλέπουμε $(p-1)! \equiv (-1)^k (k!)^2 \bmod p$

Με βάση το θεώρημα Wilson $(p-1)! \equiv -1 \bmod p \Rightarrow (-1)^k (k!)^2 \equiv -1 \bmod p$

$\Rightarrow (k!)^2 \equiv (-1)^{k+1}$. Εαν $p \equiv 1 \bmod 4$ τότε k είναι άρτιος έτσι $(k!)^2 \equiv -1$ και επιλέγω $x = k!$ είναι η λύση του $x^2+1 \equiv 0 \bmod p$

Από την άλλη υποθέτουμε $p \equiv 3 \bmod 4 \Rightarrow k = \frac{p-1}{2}$ είναι περιττός αριθμός.

Εαν x είναι η λύση του $x^2+1 \equiv 0 \bmod p$ τότε x είναι σχετικά πρώτος με p $((x,p)=1)$ Από το θεώρημα Fermat παίρνουμε $x^{p-1} \equiv 1 \bmod p$

Παρόλα αυτά $1 \equiv (x^2)^k \equiv (-1)^k \equiv -1 \pmod p$ το οποίο είναι αδύνατο αφού p είναι περιττός άρα δεν έχει λύση.

## Άσκηση 7

i) $21x \equiv 12 \pmod{33}$

$(21,33)=3=d$

$$33 = 21\cdot 1+12$$
$$21 = 12\cdot 1+9$$
$$12 = 9\cdot 1+3$$
$$9 = 3\cdot(3)+0$$

Άρα η ισοτιμία i) έχει ακριβώς 3 λύσεις modulo 33

$d/12$

$$\frac{21}{3}x \equiv \frac{12}{3} \left(\bmod \frac{33}{3}\right) \Leftrightarrow$$

$$7x \equiv 4 \pmod{11}$$

$(7,11)=1 \Leftrightarrow x \equiv 4\,7^{\phi(11)-1} \bmod 11$

$$x \equiv 4\cdot 7^{9} \pmod{11} \Leftrightarrow$$

$$x \equiv 10 \bmod 11$$

Άρα οι 3 λύσεις δίνονται από το εξής

$$x \equiv 10+11k \quad , k=0,1,2,$$

$$x \equiv 10, 21, 32 \pmod{33}$$

ii) $7x \equiv 17 \pmod{120}$

$(7,120)=1$ έχει μοναδική λύση

$\phi(120)-1 = 32-1 = 31$

$$x \equiv 17\cdot 7^{\phi(120)-1} \pmod{120}$$

$$x \equiv 17\cdot 7^{31} \pmod{120}$$

$$x \equiv 71 \pmod{120}$$

7)

iii)

$$-671x \equiv 121 \pmod{737}$$

$$-671 \equiv 66 \pmod{737}$$

$$66x \equiv 121 \pmod{737}$$

$$(737, 66) = 11 = d$$

Έχει ακριβώς <u>11 λύσεις</u> mod 737

$$\frac{66}{11}x \equiv \frac{121}{11} \left(\bmod \frac{737}{11}\right)$$

$$\boxed{6x \equiv 11 \pmod{67}}$$

$$x \equiv 11\, 6^{\phi(67)-1} \pmod{67}$$

$$x \equiv 13 \bmod 67$$

Άρα $x \equiv 13 + 67 \cdot k$, <u>$k = 0, 1, 2 \ldots, 10$</u>

$$x \equiv 13, 80, 147, 214, 281, 348, 415, 482, 549, 616, 683 \pmod{737}$$

8)

a) $\begin{cases} x \equiv 12 \mod 17 \\ x \equiv 5 \mod 21 \\ x \equiv 11 \mod 25 \end{cases}$ $\quad (17, 21, 25) = 1$

$M = 17 \times 21 \times 25 = 8925$

$M_1 = \frac{M}{17} = 525 \qquad M_2 = \frac{M}{21} = 425 \qquad M_3 = \frac{M}{25} = 357$

$525 x_1 = 1 \mod 17 \qquad 425 x_2 \equiv 1 \mod 21 \qquad 357 x_3 \equiv 1 \mod 25$

$\underline{x_1 \equiv 8 \mod 17} \qquad \underline{x_2 \equiv 17 \mod 21} \qquad x_3 = \underline{18 \mod 25}$

$x_1' = 8 \cdot 525 = \qquad x_2' = 425 \cdot 17 = \qquad x_3' = 18 \cdot 357 =$

$= 4200 \qquad = 7225 \qquad = 6426$

$x = 12 \cdot 4200 + 5 \cdot 7225 + 11 \cdot 6426 \pmod{8925}$

$= 50400 + 36125 + 70686 = 157211 \pmod{8925}$

$\Rightarrow \boxed{x \equiv 5486 \pmod{8925}}$

b)

$$\begin{cases} x \equiv 4 \mod 5 \\ x \equiv -27 \mod 22 \\ x \equiv -31 \mod 39 \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 \mod 5 \\ x \equiv 17 \mod 22 \\ x \equiv 8 \mod 39 \end{cases}$$

$$(5, 22, 39) = 1$$

$$M = 5 \cdot 22 \cdot 39 = 4290$$

$$M_1 = \frac{M}{5} = 858 \qquad M_2 = \frac{M}{22} = 195 \qquad M_3 = \frac{M}{39} = 110$$

$858 x_1 \equiv 1 \mod 5$ $\Rightarrow x_1 \equiv 2 \mod 5$

$195 x_2 \equiv 1 \mod 22$ $\Rightarrow x_2 \equiv 7 \mod 5$

$110 x_3 \equiv 1 \mod 39$ $\Rightarrow x_3 \equiv 11 \mod 39$

$x_1' = 2 \cdot 858 = 1716$

$x_2' = 7 \cdot 195 = 1365$

$x_3' = 110 \cdot 11 = 1210$

$$x = 4 \cdot 1716 + 17 \cdot 1365 + 8 \cdot 1210 =$$
$$= 6864 + 23205 + 9680 = 39749 \pmod{4290}$$

$$\Rightarrow \boxed{x \equiv 1139 \pmod{4290}}$$

c) $\begin{cases} 3x \equiv 15 \mod 55 \\ x \equiv 7 \mod 23 \\ x \equiv 11 \mod 31 \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \mod 55 \\ x \equiv 7 \mod 23 \\ x \equiv 11 \mod 31 \end{cases}$

$M = 55 \cdot 23 \cdot 31 = 39215$

$M_1 = \frac{M}{55} = 713 \quad M_2 = \frac{M}{23} = 1705 \quad M_3 = \frac{M}{31} = 1265$

$713 x_1 \equiv 1 \mod 55 \qquad 1705 x_2 \equiv 1 \mod 23 \qquad 1265 x_3 \equiv 1 \mod 31$

$\Rightarrow x_1 = 27 \mod 55 \qquad \Rightarrow x_2 \equiv 8 \mod 23 \qquad \Rightarrow x_3 \equiv 5 \mod 31$

$x_1' = 27 \cdot 713 \qquad x_2' = 8 \cdot 1705 \qquad x_3' = 5 \cdot 1265$

$x \equiv 5 \cdot 27 \cdot 713 + 7 \cdot 8 \cdot 1705 + 5 \cdot 1265 \cdot 11 \pmod{39215}$

$\Rightarrow x \equiv 96255 + 95480 + 69575 \pmod{39215}$

$\Rightarrow x = 261310 \equiv 26020 \pmod{39215}$

$\Rightarrow \boxed{x \equiv 26020 \pmod{39215}}$

## Άσκηση

Αν $m, n \in \mathbb{Z}$, $m > 1$, $n > 1$ και $\gcd(m,n) = 1$ τότε $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

**Solution**

Using Euler theorem - Fermat we have $a^{\phi(p)} \equiv 1 \pmod{p}$ $(a,p) = 1$

$$\begin{cases} m^{\phi(n)} \equiv 1 \bmod n \\ n^{\phi(m)} \equiv 1 \bmod m \end{cases} \Leftrightarrow \begin{cases} n / m^{\phi(n)} - 1 \\ m / n^{\phi(m)} - 1 \end{cases} \Leftrightarrow m \cdot n / (m^{\phi(n)} - 1) \cdot (n^{\phi(m)} - 1) =$$

$$= m^{\phi(n)} n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1 =$$

$$\Leftrightarrow \begin{cases} mn / m^{\phi(n)} \cdot n^{\phi(m)} - (m^{\phi(n)} + n^{\phi(m)} - 1) \\ m \cdot n / m^{\phi(n)} \cdot n^{\phi(m)} \end{cases}$$

$$\Rightarrow m \cdot n / m^{\phi(n)} + n^{\phi(m)} - 1$$

$$\Rightarrow \boxed{m^{\phi(n)} + n^{\phi(m)} \equiv 1 \bmod (m \cdot n)}$$

10)

Αν $d$ και $n$ θετικοί ακέραιοι τότε $\phi(d) \mid \phi(n)$ και $d/n$

<u>Λύση</u>

$d/n \Rightarrow \boxed{n = kd}$ $k \in \mathbb{Z}$

$$d = p_1^{a_1} \cdots p_k^{a_k}$$

$$\phi(d) = p^{a_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_k^{a_k - 1}(p_k - 1)$$

Έστω $l = k \prod_{t=1}^{k} \frac{1}{p_t^{m_t}}$ $\quad p_t^{m_t} / k$

Έτσι $n = p_1^{a_1 + m_1} p_2^{a_2 + m_2} \cdot \ldots \cdot p_s^{a_k + m_k} \cdot l$

$$\varphi(n) = \varphi(p_1^{a_1 + m_1}) \cdot \ldots \cdot \varphi(p_k^{a_k + m_k}) \varphi(l) =$$

$$= p^{a_1 + m_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_k^{a_k + m_k - 1}(p_k - 1) \varphi(l) =$$

$$= (p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}) \varphi(d) \varphi(l)$$

$$\Rightarrow \varphi(d) / \varphi(n)$$

Άσκηση 1

(Μέρος 2ο)

Να υπολογιστεί το υπόλοιπο της διαίρεσης $12^{23} 19^{37}$ με το 8

Λύση

$12 \equiv 4 \mod 8 \Leftrightarrow$

$12^2 \equiv 16 \mod 8 \Leftrightarrow$

$12^2 \equiv 0 \mod 8 \Leftrightarrow$

$(12^2)^{10} \equiv 0^{10} \mod 8 \Leftrightarrow$

$12^{20} \equiv 0 \mod 8 \Leftrightarrow$

$12^{20} 12^3 \equiv 0 \mod 8 \Leftrightarrow$

$12^{23} \equiv 0 \mod 8$ (1)

Άρα χωρίς να χρειαστεί να βρούμε το υπόλοιπο του $19^{37}$ με το 8 και από την (1) και μόνο το υπόλοιπο του $12^{23} 19^{37}$ με το 8 είναι μηδέν δηλαδή,

$12^{23} 19^{37} \equiv 0 \mod 8$

## Άσκηση 2

Ας υποθέσουμε ότι $a, b, k \in \mathbb{Z}$ με $k \neq 0$ και $d = \gcd(n,k)$ τότε

$$ka \equiv kb \bmod n \Leftrightarrow a \equiv b \left(\bmod \frac{n}{d}\right)$$

### Λύση

($\Rightarrow$) Από $ka \equiv kb \pmod n$ έπεται ότι $n / k(a-b)$ οπότε $\frac{n}{d} \Big| \frac{k}{d}(a-b)$

Αλλά $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ Άρα $\frac{n}{d} \Big| (a-b) \Leftrightarrow a \equiv b \left(\bmod \frac{n}{d}\right)$

($\Leftarrow$) $a \equiv b \left(\bmod \frac{n}{d}\right) \Leftrightarrow \frac{n}{d} \Big| (a-b) \Leftrightarrow n / (a-b)d \Leftrightarrow$

$n / (a-b)dk' \Leftrightarrow n / (a-b)k \Leftrightarrow n / (ka-kb) \Leftrightarrow$

$ka \equiv kb \pmod n$

3) Αν $a$ και $b$ είναι ακέραιοι που δεν διαιρούνται από το 3, να δειχθεί ότι ο ακέραιος $a^2+b^2$ δεν είναι τέλειο τετράγωνο ακεραίου

Λύση

Έχουμε $a^2+b^2 \equiv 0$ ή $1$ ή $2 \mod 3$

Εάν $a^2+b^2 \equiv 0 \mod 3$, $a, b \not\equiv 0 \mod 3$ και $a^2, b^2 \not\equiv 0 \mod 3$

$a^2 \equiv 1 \mod 3$, $b^2 \equiv 2 \mod 3$

Άρα $a$ ρίζα της εξίσωσης $x^2 \equiv 1 \mod 3$ και $b$ ρίζα της $x^2 \equiv 2 \mod 3$

Άτοπο αφού $1 = \left(\frac{2}{3}\right) \equiv 2^{\frac{3-1}{2}} \mod 3 \equiv 2 \mod 3$ <u>άτοπο</u>

Έστω ότι $a^2+b^2 \equiv 1 \mod 3 \Longleftrightarrow$

$a^2 \equiv b^2 \equiv 2 \mod 3$ που είναι <u>αδύνατο</u>

Ως εκτός $a^2+b^2 \equiv 2 \mod 3 \Longleftrightarrow$

$a^2 \equiv b^2 \equiv 1 \mod 3$

Έχουμε ότι η λύση της $a^2+b^2 \equiv x^2 \mod 3$ και αφού

$n^2 \equiv 1 \mod 3$ έχουμε $\left(\frac{2}{3}\right) \equiv 1$, <u>άτοπο</u>

4) Να δειχθεί ότι για κάθε ακέραιο $n$ ισχύει $2730 \mid n^{13} - n$

Λύση

Έχουμε τον αριθμό $2730$ ο οποίος αναλύεται σε γινόμενο πρώτων παραγόντων

$$2730 = 2 \times 3 \times 5 \times 7 \times 13$$

Από Euler-Fermat θεώρημα έχουμε:

$$n^{\varphi(p)} \equiv 1 \mod p \quad , \quad (n,p) = 1$$

- $\varphi(2) = 1$
- $\varphi(3) = 2$
- $\varphi(5) = 4$
- $\varphi(7) = 6$
- $\varphi(13) = 12$

$\Longrightarrow n^{\varphi(2)} = n \equiv 1 \mod 2 \Longrightarrow \underline{n^{13} \equiv n \mod 2}$ (1)

$\Longrightarrow n^{\varphi(3)} = n^2 \equiv 1 \mod 3 \Longrightarrow (n^2)^6 \cdot n \equiv n \mod 3 \Rightarrow \underline{n^{13} \equiv n \mod 3}$ (2)

$\Longrightarrow n^{\varphi(5)} = n^4 \equiv 1 \mod 5 \Longrightarrow (n^4)^3 \cdot n \equiv 1^3 \cdot n \mod 5 \Rightarrow \underline{n^{13} \equiv n \mod 5}$ (3)

$\Longrightarrow n^{\varphi(7)} = n^6 \equiv 1 \mod 7 \Longrightarrow (n^6)^2 \cdot n \equiv 1^2 \cdot n \mod 7 \Rightarrow n^{13} \equiv n \mod 7$ (4)

$\Longrightarrow n^{\varphi(13)} = n^{12} \equiv 1 \mod 13 \Longrightarrow n^{12} \cdot n \equiv n \mod 13 \Rightarrow n^{13} \equiv n \mod 13$ (5)

Οι (1), (2), (3), (4), (5) γράφονται:

$$\begin{cases} 2 \mid n^{13} - n \\ 3 \mid n^{13} - n \\ 5 \mid n^{13} - n \\ 7 \mid n^{13} - n \\ 13 \mid n^{13} - n \end{cases} \xRightarrow{\text{γινόμενο}} \underline{2 \times 3 \times 5 \times 7 \times 13 \mid n^{13} - n} \Longleftrightarrow \boxed{2730 \mid n^{13} - n}$$

$\blacksquare$

5) Να δειχθεί ότι ο αριθμός $\dfrac{7\cdot 1968^{1968} - 3\cdot 68^{78}}{10}$ είναι ακέραιος

Λύση

Αρκεί να δείξουμε ότι $A = 7\cdot 1968^{1968} - 3\cdot 68^{78}$

$10 \mid A$

$10 = 2\cdot 5$ και $(2,5)=1$ $*$

- $7\cdot 1968^{1968} - 3\cdot 68^{78} = 2K,\ K\in\mathbb{Z}$

$\Rightarrow 2 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$ (1)

Μικρό θεώρημα Fermat $\underline{a^{p-1}\equiv 1 \bmod p}$

$\Rightarrow 3^4 \equiv 1 \pmod 5$

$1968^{1968} \equiv 3^{1968} \equiv (3^4)^{492} \equiv 1 \bmod 5$

$68 \equiv 3 \bmod 5 \Rightarrow$

$68^{78} \equiv 9 \equiv 4 \bmod 5$

$\Rightarrow 7\cdot 1968^{1968} - 3\cdot 68^{78} \equiv 7 - 3\cdot 4 \equiv -5 \equiv 0 \bmod 5$

$\Rightarrow 5 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$ (2)

$A \overset{(1)}{\underset{(2)}{\Longrightarrow}} \underline{10 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}}$.

## Άσκηση 6

Έστω $f$ μια πολλαπλασιαστική συνάρτηση, Να δειχθεί ότι η συνάρτηση $F$ που ορίζεται από τη σχέση $F(n) = \sum_{d|n} f(d)$ για κάθε ακέραιο $n>0$ είναι πολλαπλασιαστική

### Λύση

Αφού η $f$ πολλαπλασιαστική άρα έστω $n = n_1 n_2$
$(d_1, d_2) = 1$

$$F(n) = F(n_1 n_2) = \sum_{d|n_1 n_2} f(d_1 d_2) = \sum_{d_1|n_1} f(d_1) \sum_{d|n_2} f(d_2) = F(n_1) F(n_2)$$

Άρα η $F(n)$ είναι πολλαπλασιαστική

## Άσκηση 7

Ας υποθέσουμε ότι $a, b, n \in \mathbb{Z}$ με $\gcd(a,n) = \gcd(b,n) = 1$. Αν $\gcd(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$

Τότε να δειχθεί ότι:

$$\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\,\mathrm{ord}_n(b)$$

### Λύση

Επειδή $\gcd(a,n) = \gcd(b,n) = 1$, έπεται ότι ορίζονται οι τάξεις $\mathrm{ord}_n(a)$ και $\mathrm{ord}_n(b)$ των $a$ και $b$ mod $n$

Έστω $\mathrm{ord}_n(a) = r$ και $\mathrm{ord}_n(b) = s$ και $\mathrm{ord}_n(ab) = t$ υποθέτουμε ότι $\gcd(r,s) = 1$

Έχουμε $(ab)^{rs} = a^{rs} \cdot b^{rs} = (a^r)^s \cdot (b^r)^s \equiv 1^s \cdot 1^r \equiv 1 \pmod n \Rightarrow t \mid rs$ (1)

Επίσης

$(ab)^t \equiv 1 \bmod n \Rightarrow (ab)^{rt} \equiv 1 \bmod n \Rightarrow a^{rt} b^{rt} \equiv 1 \bmod n \Rightarrow (a^r)^t (b^r)^t \equiv 1 \bmod n$

$\Rightarrow b^{rt} \equiv 1 \bmod n \Rightarrow s \mid rt \underset{(r,s)=1}{\Longrightarrow} s \mid t$ (*)

Όμοια

$(ab)^t \equiv 1 \bmod n \Rightarrow (ab)^{st} \equiv 1 \bmod n \Rightarrow a^{st} b^{st} \equiv 1 \bmod n \Rightarrow a^{st} (b^s)^t \equiv 1 \bmod n \Rightarrow$

$\Rightarrow a^{st} \equiv 1 \bmod n \Rightarrow r \mid st \underset{(r,s)=1}{\Longrightarrow} r \mid t$ (**)

Επειδή $(s,r) = 1$ Από (*), (**) παίρνουμε ότι: $rs \mid t$ (2)

Τέλος με βάση τις (1) και (2) έχουμε ότι $t = r \cdot s \Leftrightarrow$

$$\boxed{\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\,\mathrm{ord}_n(b)}$$

## Άσκηση 8

Ας υποθέσουμε ότι $a, b, n \in \mathbb{Z}$ με $n > 1$ και $ab \equiv 1 \bmod n$. Να δειχθεί ότι $\mathrm{ord}_n(a) = \mathrm{ord}_n(b)$

## Λύση

Επειδή $ab \equiv 1 \bmod n$ έχουμε $n \mid ab-1$

Έστω $d = (a,n)$ Τότε

$$\begin{cases} d \mid n \\ d \mid a \end{cases} \Rightarrow \begin{cases} d \mid n \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid ab-1 \\ d \mid ab \end{cases} \Rightarrow d \mid 1 \Rightarrow d = (a,b) = 1$$

δηλαδή και το $(b,n) = 1$

Έστω $\mathrm{ord}_n(a) = r$ $\mathrm{ord}_n(b) = s$

$$a^r \equiv 1 \pmod n \text{ και } b^s \equiv 1 \pmod n$$

Έχουμε $a^r \equiv 1 \bmod n \Rightarrow a^r b^r \equiv b^r \bmod n$

$$\Rightarrow (ab)^r \equiv b^r \bmod n$$

$$\Rightarrow 1^r \equiv 1 \equiv b^r \bmod n$$

$$\Rightarrow b^r \equiv 1 \pmod n$$

άρα $\mathrm{ord}_n(b) = s \mid r$ (1)

$b^s \equiv 1 \bmod n \Rightarrow a^s b^s \equiv a^s \bmod n$

$$\Rightarrow (ab)^s \equiv a^s \bmod n$$

$$\Rightarrow 1^s \equiv 1 \equiv a^s \bmod n$$

$$\Rightarrow a^s \equiv 1 \bmod n$$

άρα $\mathrm{ord}_n(a) = r \mid s$ (2)

Από (1) και (2) έχουμε ότι $\mathrm{ord}_n(a) = r = s = \mathrm{ord}_n(b)$

## Άσκηση 11

Αν $p$ πρώτος $p>2$ να δειχθεί ότι ισχύουν οι σχέσεις

(α) $$\left(\frac{3}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod{12} \\ -1, & p \equiv \pm 5 \pmod{12} \end{cases}$$

## Λύση

Με βάση τον νόμο της τετραγωνικής αντιστροφής έχουμε

$$\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

Για να βρούμε το $\left(\frac{p}{3}\right)$ χρειάζεται να ξέρουμε την τιμή του $p \bmod 3$ και να προσδιορίσουμε το $(-1)^{\frac{p-1}{2}}$ χρειάζεται να ξέρουμε την τιμή $\frac{p-1}{2} \bmod 2$ ή την τιμή το $p \bmod 4$. Επομένως θεωρούμε το $p \bmod 12$. Υπάρχουν μόνο τέσσερις περιπτώσεις να επιλύσουμε $p \equiv 1, 5, 7$ ή $11 \pmod{12}$ ενώ οι υπόλοιπες (8) αποκλείονται επειδή ο $p$ είναι περιττός πρώτος.

Case 1 $p \equiv 1 \bmod 12$. Στην περίπτωση αυτή είναι $p \equiv 1 \bmod 3$, οπότε $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$

Επίσης, $p \equiv 1 \bmod 4$ οπότε $\frac{p-1}{2}$ είναι άρτιος άρα $\left(\frac{3}{p}\right) = 1$

Case 2 $p \equiv 5 \bmod 12$. Σε αυτή την περίπτωση είναι $p \equiv 2 \bmod 3$, οπότε $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$. Πάλι ο $\frac{p-1}{2}$ είναι άρτιος, επειδή $p \equiv 3 \bmod 4$, άρα $\left(\frac{3}{p}\right) = -1$

Case 3 $p \equiv 7 \bmod 12$. Σε αυτή την περίπτωση $p \equiv 1 \bmod 3$ οπότε $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Επίσης $\frac{p-1}{2}$ είναι περιττός επειδή $p \equiv 3 \bmod 4$ επομένως $\left(\frac{3}{p}\right) = -1$

Case 4 $p \equiv 11 \bmod 12$. Σε αυτή την περίπτωση το $p \equiv 2 \bmod 3$, οπότε $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$

και εδώ ο $\frac{p-1}{2}$ είναι περιττός επειδή $p \equiv 1 \bmod 4$ άρα $\left(\frac{3}{p}\right) = 1$

Άρα με βάση τις case 1, case 2, case 3, case 4 παίρνουμε ότι

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod{12} \\ -1, & p \equiv \pm 5 \pmod{12} \end{cases}$$

b) $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$

Λύση

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \dots + \left(\frac{p-2}{p}\right) + \left(\frac{p-1}{p}\right) =$$

$$= 1 + (-1)^{\frac{p^2-1}{8}} + \dots$$

Εδώ υπάρχουν τόσα τετραγωνικά υπόλοιπα που μας δίνει +1

και άλλα τόσα μη-τετραγωνικά υπόλοιπα που μας δίνει −1

Άρα εάν ~~αθροίσουμε~~ αθροίσω τα τετραγωνικά και μη-τετραγωνικά μας δίνουν $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$

## Άσκηση 13

α) Να υπολογιστούν τα σύμβολα Jacobi:

$$\left(\frac{102}{231}\right) = \left(\frac{2\ 51}{231}\right) = \left(\frac{2}{231}\right)\left(\frac{51}{231}\right) = (-1)^{\frac{231^2-1}{8}}\left(\frac{51}{231}\right) = (-1)^{6670}\left(\frac{51}{231}\right) =$$

$$= \left(\frac{51}{231}\right) = (-1)^{\frac{231-1}{2}\cdot\frac{51-1}{2}}\left(\frac{231}{51}\right) = (-1)^{115\cdot 25}\left(\frac{27}{51}\right) =$$

$$= -1\left(\frac{27}{51}\right) = -\left(\frac{27}{51}\right) = -\left(\frac{32\cdot 3}{51}\right) = -\left(\frac{32}{51}\right)\cdot\left(\frac{3}{51}\right) = -\left(\frac{3}{51}\right) =$$

$$= -(-1)^{\frac{51-1}{2}\cdot\frac{3-1}{2}}\left(\frac{51}{3}\right) = -(-1)^{25}\cdot\left(\frac{0}{3}\right) = \left(\frac{0}{3}\right) = 0$$

b) $\left(\frac{131}{1999}\right) = (-1)^{\frac{1999-1}{2}\cdot\frac{131-1}{2}}\left(\frac{1999}{131}\right) = (-1)^{\overset{64{,}975}{\overset{\shortparallel}{999\cdot 65}}}\left(\frac{34}{131}\right) =$

$= -\left(\frac{34}{131}\right) = -\left(\frac{2\cdot 17}{131}\right) = -\left(\frac{2}{131}\right)\left(\frac{17}{131}\right) = -(-1)^{\frac{131^2-1}{8}}\cdot\left(\frac{17}{131}\right) =$

$= -(-1)^{2145}\cdot\left(\frac{17}{131}\right) = \left(\frac{17}{131}\right) = (-1)^{\frac{131-1}{2}\cdot\frac{17-1}{2}}\cdot\left(\frac{131}{17}\right) =$

$= (-1)^{65\cdot 8 = 520}\left(\frac{12}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{2^2}{17}\right)\cdot\left(\frac{3}{17}\right) =$

$= 1\cdot\left(\frac{3}{17}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right) = (-1)^{8}\left(\frac{-1}{3}\right) =$

$= \left(-\frac{1}{3}\right) = (-1)^{\frac{3-1}{2}} = (-1)^1 = -1$

c) $\left(\frac{1704}{3535}\right) = \left(\frac{2\ 852}{3535}\right) = \left(\frac{2}{3535}\right)\left(\frac{852}{3535}\right) = (-1)^{\frac{3535^2-1}{8}}\left(\frac{852}{3535}\right) =$

$= (-1)^{1562028}\left(\frac{852}{3535}\right) = \cancel{(-1)^{\frac{852-1}{2}\cdot\frac{3535-1}{2}}\left(\frac{3535}{852}\right)} \neq$ $\cancel{\frac{124}{852}}$

$= \left(\frac{2\cdot 426}{3535}\right) = \left(\frac{2}{3535}\right)\left(\frac{426}{3535}\right) = \left(\frac{426}{3535}\right) = \left(\frac{2}{3535}\right)\left(\frac{213}{3535}\right) =$

$= \left(\frac{213}{3535}\right) = (-1)^{\frac{213-1}{2}\cdot\frac{3535-1}{2}}\left(\frac{3535}{213}\right) = \left(\frac{127}{213}\right) = (-1)^{\frac{213-1}{2}\cdot\frac{127-1}{2}}\left(\frac{213}{127}\right) =$

$= \left(\frac{86}{127}\right) = \left(\frac{2\cdot 43}{127}\right) = \left(\frac{2}{127}\right)\cdot\left(\frac{43}{127}\right) = -\left(\frac{41}{43}\right) = -\left(\frac{2}{41}\right) = -\left(\frac{1}{41}\right) = -1$

d) $\left(\frac{2166}{31625}\right) = \left(\frac{2 \cdot 1083}{31625}\right) = \left(\frac{2}{31625}\right) \cdot \left(\frac{1083}{31625}\right) = (-1)^{\frac{31625^2-1}{8}} \left(\frac{1083}{31625}\right) =$

$= \left(\frac{1083}{31625}\right) = (-1)^{\frac{1083-1}{2} \cdot \frac{31625}{2}} \left(\frac{31625}{1083}\right) = \left(\frac{218}{1083}\right) = \left(\frac{2 \cdot 109}{1083}\right) = \left(\frac{2}{1083}\right)\left(\frac{109}{1083}\right)$

$= (-1)^{\frac{1083^2-1}{8}} \left(\frac{109}{1083}\right) = -\left(\frac{102}{109}\right) = \left(\frac{51}{109}\right) = \left(\frac{7}{51}\right) = -\left(\frac{2}{7}\right) = -\left(\frac{1}{7}\right) = \underline{-1}$

9) a) if $p = 4q+1$ where $q$ is an odd prime then $2$ is primitive root

Solution

we first If $t$ is the order of $2$ then $t$ divides $p-1 = 4q$ so $t = 1, 2, 4, q, 2q$ or $4q$. Now if $t = 1, 2$ or $4$ then $2^4 \equiv 1 \bmod p$, so that $p$ divides $15$. But then $p = 3$. which is too small or $p = 5$ so that $q = 1$, which is not prime.

otherwise either $t = 4q$ or $t \mid (2q)$, so that it suffices to show $2^{2q} \not\equiv 1 \bmod p$

Suppose that $q = 2k+1$ Then

$$p = 4q+1 = 4(2k+1)+1 = 8k+5$$

Therefore

$$2^{2q} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) \bmod p = -1$$

as $p \equiv 5 \bmod 8$

(12)

i) $x^2 - 6x - 13 \equiv 0 \bmod 127$

Solution

127 is prime

$\cancel{x^2 - 2 \cdot 3x - 3^2 - 4 \equiv 0 \bmod 127}$

$\cancel{x^2 - 6x + 9}$

$x^2 - 6x - 13 = x^2 - 6x - 13 + 22 \equiv 22 \bmod 127 \Leftrightarrow$

$x^2 - 6x - 13 + 22 \equiv 22 \bmod 127 \Leftrightarrow$

$x^2 - 6x + 9 \equiv 22 \bmod 127$

$(x-3)^2 \equiv 22 \bmod 127$

Θέτω $y = x - 3$ Άρα $y^2 \equiv 22 \bmod 127$

Υπολογίζουμε σύμβολο του Legendre για να δούμε αν η παραπάνω ισοτιμία και $p = 127$

έχει $\left(\frac{22}{127}\right) = \left(\frac{1}{127}\right)\left(\frac{11}{127}\right) = 1 \cdot \left(\frac{11}{127}\right) = (-1)^{\frac{11-1}{2} \cdot \frac{127-1}{2}} \left(\frac{127}{11}\right) = 1$

Άρα η $y^2 \equiv 22 \bmod 127$ έχει λύση

Άρα η εξίσωση $y^2 \equiv 22 \bmod 127$ έχει δυο λύσεις

$y \equiv 28 \bmod 127$ και $y \equiv 99 \bmod 127$

Άρα $y = x - 3$ $\begin{cases} x = y + 3 = 28 + 3 = 31 \\ x = y + 3 = 99 + 3 = 102 \end{cases}$

Άρα $x \equiv 31, 102 \bmod 127$

ii) $x^2+6x-154 \equiv 0 \bmod 399$

<u>Solution</u>

$$x^2+6x-154 = x^2+6x+9-163 \equiv 0 \bmod 399 \Leftrightarrow$$

$$x^2+6x+9 \equiv 163 \bmod 399 \Leftrightarrow$$

$$(x+3)^2 \equiv 163 \bmod 399$$

$y = x+3$ $\qquad y^2 \equiv 163 \bmod 399$

Άρα
$$\begin{cases} y \equiv 178 \bmod 399 \\ y \equiv 31 \bmod 399 \\ y \equiv 235 \bmod 399 \\ y \equiv 88 \bmod 399 \\ y \equiv 331 \bmod 399 \\ y \equiv 164 \bmod 399 \\ y \equiv 368 \bmod 399 \\ y \equiv 221 \bmod 399 \end{cases}$$

Άρα $x = y-3 \Leftrightarrow x \equiv 175, 28, 232, 85, 308, 161, 365, 218 \bmod 399$

Άσκηση 15

$x^2 + 4322 \equiv 0 \mod 10961$

Solution

Έχουμε ότι $10961 = 97 \cdot 113$

$x^2 \equiv -4322 \mod 10961 \Leftrightarrow$

$x^2 \equiv 6639 \mod 10961$

$x^2 \equiv 43 \mod 97$ και $x^2 \equiv 85 \mod 113$

Θα βρούμε σύμβολο του Legendre για να δούμε εάν επιδέχονται αρχικά

$\left(\frac{43}{97}\right) = 1$ $\left(\frac{85}{113}\right) = 1$

So, the two quadratic congruences are solvable:

$113 \equiv 97 \equiv 1 \mod 4$

Άρα η εξίσωση έχει λύση μέσω Tonelli Shanks Algorithm

Λύνοντας τις άνωθε παίρνουμε ότι:

$x = 10113$

$x = 10792$

$x = 169$

$x = 848$

Άσκηση 1

$x^2 + 4322 \equiv 0 \mod 10961$

Solution

Έχουμε ότι $10961 = 97 \cdot 113$

$x^2 \equiv -4322 \mod 10961 \Leftrightarrow$

$x^2 \equiv 6639 \mod 10961$

$x^2 \equiv 43 \mod 97$ και $x^2 \equiv 85 \mod 113$

Θα βρούμε σύμβολο του Legendre για να δούμε εάν επιδέχονται αρχικά

$\left(\frac{43}{97}\right) = 1$ $\left(\frac{85}{113}\right) = 1$

So, the two quadratic congruences are solvable:

Λύνοντας τις άνωθε παίρνουμε ότι:

$x = 10113$

$x = 10792$

$x = 169$

$x = 848$

$113 \equiv 97 \equiv 1 \mod 4$

Άρα επίσης έχουμε λύση με Tonelli Shanks Algorithm

## Exercise 2

Για το $F_{16}$:

Κατασκευάζω το σώμα $F_{16}$ με $16 = 2^4$ στοιχεία

Παρατηρώ $x^4+x+1 \in F_2[x]$ είναι ανάγωγο και $f(0)=f(1)=1$

και δεν έχει ρίζες επί του $F_2$. Άρα $F_{16} = F_2[x]/\langle x^4+x+1\rangle = \{0, 1, x, x+1, x^2, x^2+1, x^2+x,$

$, x^2+x+1, x^3, x^3+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x+1, x^3+x^2+x\}$.

Αν με α συμβολίσω το x modulo $x^4+x+1$ τότε το α και κορφές διανύσματος είναι $(0,0,1,0)$.

Το υπόλοιπο θα είναι $ax^3+bx^2+cx+d$

$a^2 \to x^2 \Rightarrow a^2=(0,1,0,0)$

$a^3 \to x^3 \Rightarrow a^3=(1,0,0,0)$

$a^4 \to x^4 \Rightarrow a^4=(0,0,1,1)$

$a^5 = a^2+a \Rightarrow a^5=(0,1,1,0)$

$a^6 = a^3+a^2 = (1,1,0,0)$

$a^7 = a^4+a^3 = (1,0,1,1)$

$a^8 = a^4+a^2+a = (0,1,0,1)$

$a^9 = a^4+a^2 = (1,0,1,0)$

$a^{10} = a^4+a^2 = (0,1,1,1)$

$a^{11} = a^3+a^2+a = (1,1,1,0)$

$a^{12} = a^4+a^3+a = (1,1,1,1)$

$a^{13} = a^4+a^3+a^2+a = (1,1,0,1)$

$a^{14} = a^4+a^3+a = (1,0,0,1)$

$a^{15} = a^4+a = (0,1,0,1)$

Έχω ότι $(x-a)(x-a^2)(x-a^4)(x-a^8) = x^4+x+1$

$(x-a^3)(x-a^6)(x-a^9)(x-a^{12}) =$

$= x^4+x^3+x^2+1$

$b=a^3$ άρα $1=(0001)$, $b=(1000)$, $b^2=(1100)$

$b^3=(1010)$, $b^4=(1111)$

Άρα $b^4+b^3+b^2+b+1=0$. $b=a^3\neq 1 \Rightarrow b^5=(a^3)^5=a^{15}=1$

Το b είναι μια 5-ρίζα του μοναδιαίου ρίζαρα

$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$

Για το $F_{25}$

Θεωρούμε πολυώνυμο $x^2-2 \in \mathbb{Z}_5[x]$. Το πολυώνυμο είναι ανάγωγο στο πρώτο $F_5$ γιατί βαθμό 2 και κανένα στοιχείο του $\mathbb{Z}_5$ δεν είναι ρίζα του

$$F_5[x]/(x^2-2) = \{0, 1, 2, 3, 4, x, x+1, x+2, x+3, x+4, 2x, 2x+1, 2x+2, 2x+3, 2x+3, 2x+4, 3x, 3x+1, 3x+2, 3x+3, 3x+4, 4x, 4x+1, 4x+2, 4x+3, 4x+4\}$$

Με βάση τον αλγόριθμο του Gauss για τον πρωτογενή ρίζα έχουμε

$a_1 = x$

$a_1^0 = 1$, $a_1^1 = x$, $a_1^2 = x^1 = 2$, $x^3 = 2x$, $x^4 = 4$, $x^5 = 4x$, $x^6 = 3$, $x^7 = 3x$

$x^8 = 1$

$\mathrm{ord}(F_{25}) = 24$

διαλέγουμε $b$ που δεν είναι δύναμη του $a_1$ έστω $x+1$

$b, b^2 = 2x+3, b^3 = 2, b^4 = 2x+2, b^5 = 4x+1, b^6 = 4, b^7 = 4x+4$

$b^8 = 3x+2, b^9 = 3, b^{10} = 3x+3, b^{11} = x+4, b^{12} = 1$

Το $b$ έχει τάξη 12 άρα δεν έχει τετραγωνική ρίζα

ψάχνουμε $d, e$ με $d/t_1 = 8$ και $e/s = 12$ ώστε $(d,e) = 1$

$d \cdot e = [t_1, s] = (8, 12) = 24$, $d = 8$, $e = 3$

Άρα $a_2 = a_1^{t_1/d} b^{s/e}$

$a_2 = a_1^{8/8} b^{12/3} = a_1 b^4 = 2x+4$

Σε μια ομάδα με στοιχεία $A, B \Rightarrow BA = AB$ και τάξη $m, n$ $(m,n) = 1$

η τάξη του γινομένου είναι $mn$

Άρα το $2x+4$ είναι μια πρωτογενής ρίζα της μονάδας στο $F_{25}$.

Exercise 3

Find the smallest Fermat number to the base 2 and 5.

Solution

So, from theory we have the smallest Fermat pseudoprime with base 2 is 341 odd  341 is a composite number  $341 = 11 \times 31$ (Poulet number)

$$2^{341-1} \equiv 1 \mod 341 \qquad (2, 341) = 1$$

From the definition we have: a number $n$ is an $a$-pseudoprime if $n$ is composite and $a^{n-1} \equiv 1 \mod n$

$a = 5$

$n = 4 = 2 \cdot 2$  $(5, 4) = 1$

$$5^{4-1} = 5^3 \equiv 1 \mod 4$$

Hence, the smallest pseudoprime are 341 for the base 2 and 4 for the base 5.

Of course as we can try we will find and others pseudoprimes for the bases 2 and 5

but if we add the requierment to $n$ to be an odd composite number then the smallest is $217 = 7 \times 31$

$$5^{216} \equiv 1 \mod 217 \qquad (5, 217)$$

Exercise 4

from the theory we know an n odd composite integer is called Pseudoprime of Fermat to the base $a$ if $a^{n-1} \equiv 1 \bmod n$ $(a,n)=1$

So, $n = 15$

$a^{15-1} = a^{14} \equiv 1 \bmod n \Leftrightarrow a^{14} \equiv 1 \bmod 15$ $(a, 15) = 1$

Hence the possible a are: ~~1, 2, 4, 7, 11, 14~~ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14.

We start to try

- $1^{14} \equiv 1 \bmod 15$
- $2^{14} \not\equiv 1 \bmod 15$
- $4^{14} \equiv 1 \bmod 15$
- $7^{14} \not\equiv 1 \bmod 15$
- $11^{14} \equiv 1 \bmod 15$
- $14^{14} \equiv 1 \bmod 15$

So the bases are 1, 4, 11, 14.

## Exercises

Let $n = pq$ ; where $p \neq q$ , $p, q$ primes and $d = \gcd(p-1, q-1)$. Prove that $n$ is a Fermat pseudoprime to base $b$ if and only if:

$$b^d \equiv 1 \bmod n$$

## solution

($\Rightarrow$) $pq$ is a pseudoprime, we have $b^{pq-1} \equiv 1 \bmod pq$

from Fermat $b^{q-1} \equiv 1 \bmod q$

Combining this with $b^{pq-1} \equiv 1 \bmod q$, we get $b^{p-1} \equiv 1 \bmod q$

Therefore $b^{\gcd(p-1, q-1)} \equiv 1 \bmod q$

In the same way $b^{\gcd(p-1, q-1)} \equiv 1 \bmod p$

So, $b^d \equiv b^{\gcd(p-1, q-1)} \equiv 1 \bmod pq \equiv 1 \bmod n$

$\Rightarrow b^d \equiv 1 \bmod n$

($\Leftarrow$) $b^d \equiv 1 \bmod n$ is pseudoprime is the definition

$\blacksquare$

Exercise 6

Using Fermat Criterion prove that the numbers 1111 and 2047 are composite numbers

Solution

We follow the algorithm:

- Step 1 choose a random integer $a \in \{2, 3, \dots, n-1\}$
- Step 2 compute $\gcd(a,n)$ if it is greater than 1, then stop output n is composite. Otherwise go to the next steps
- Step 3 compute $a^{n-1} \bmod n$
  - if $a^{n-1} \not\equiv 1 \bmod n$, then stop output n is composite
  - if $a^{n-1} \equiv 1 \bmod n$, then n may be a prime or composite number

  Do one of the following
  - Return to step 1 and repeat the process with a new a
  - output n is Probably Prime and stop

- let $a=2$ $(2, 1111) = 1$

  $2^{1110} \not\equiv 1 \bmod 1111$ so from above algorithm 1111 is a composite number

- let $a=2$ $(2, 2047) = 1$

  $2^{2046} \equiv 1 \bmod 2047$ I dot know if is prime or composite

let $a=3$ $(3, 2047) = 1$

$3^{2046} \not\equiv 1 \bmod 2047$ So 2047 is composite number

Exercise 7

The 561 is a Carmichael number of the form $3pq$ and is the smallest Carmichael where $p, q$ distinguish primes.

Let $n = 3pq$ with $q > p$ odd primes be a carmichael number. Using the criterion of Korselt's, we obtain $(p-1)(3pq-1) = 3(p-1)q + 3q - 1$. So $(p-1)(3q-1) \Rightarrow (p-1)a = 3q-1 \ \forall a \in \mathbb{Z}$. Since $q > p$ we must have $a \geq 4$. Similarly, $\exists b \in \mathbb{Z}$ such that $(q-1)a = 3p-1$. From these two equations we have

$$p = 2b + ab - q - 3ab = 1 + 2b + 6ab - q \quad (1)$$

$$q = 2a + ab - 3ab - q \quad (2)$$

Since $p > 3$ odd prime, therefore $4(ab-q) \leq 2b+6$ reduces to $b(2a+1) \leq 21$

Now $a \geq 4 \Rightarrow b \leq 3$ then

$$4(ab-q) \leq 2b+6 \leq 12 \Rightarrow ab \leq 21 \cdot 4 \Rightarrow a \leq 5$$

Hence, $a = 4$ or $5$ if $b = 3$, then the denominator of (2) is multiple of 3. The numerator is multiple of 3 which is impossible as there $\nexists$ any $a$ divisible by 3. Thus $b = 1$ or $2$. The denominator of equation (2) must be positive so $ab > q$. Thus the only possible values for $a$ and $b$ is 5 and 2 respectively which gives $p = 11$, $q = 17$. So $561 = 3 \cdot 11 \cdot 17$ is the only Carmichael number of the form $3pq$, where $p$ and $q$ primes

And the Carmichael number of the form $5pq$ are:

$$1105 = 5 \cdot 13 \cdot 17$$

and

$$2465 = 5 \cdot 17 \cdot 29$$

The proof is the same as above.

Assume $r > q$. Applying Korselt's Criterion we get $(q-1)(pqr-1) = (q-1)pn + pr - 1$. Therefore $(q-1)(pr-1) \Rightarrow pr-1 = a(q-1)$ for some $a \in \mathbb{Z}$.

Similarily $pq-1 = b(r-1)$ for $b \in \mathbb{Z}$. Since $r > q$ so $a > b$. Solving the last two equations for $q$ and $r$:

$$r = \frac{p(a-1)+a(b-1)}{ab-p^2}, \quad q = \frac{p(b-1)+b(a-1)}{ab-p^2}$$

Because the last fraction must be integer

$$ab - p^2 \leq p^2 + pb - p - b \Longleftrightarrow$$

$$a(b-1) \leq 2p^2 + p(b-1) \Longleftrightarrow$$

$$a-1 \leq 2p^2 + \frac{p(b-1)}{b} \leq 2p^2 + p$$

So $\exists$ only finite values for $a$. ~~the~~ Likewise, the same ~~inequality~~ inequality gives us

$$b(a-1) \leq 2p^2 + p(b-1) \Rightarrow b(a-1-p) \leq 2p^2 - p$$

Since $a > b$ and denominator of expressions for must be positive, $a \geq p+1$

Now $a = p+1$ gives

$$(p+1)(q-1) = pq - p + q - 1 \Rightarrow pr - 1 \Rightarrow p \mid q \text{ a contradiction}$$

Therefore $a > p+1 \Rightarrow a-p-1 > 0$. The last inequality gives us

$$b \leq b(a-p-1) \leq 2p^2 - p$$

which shows $\exists$ finitely many values of $b$. Because $a, b$ determine $q, r$ respectively, therefore there are only a finite number of Carmichael number of the form $n = rpq$.

## Exercise 8

$F_5 = 2^{32} + 1 = 4294967296 + 1 = 4294967297$

If I prove that Fermat number $F_5$ is divisible by 641 we see that $F_5$ is a composite number

Let $a = 2^7$, $b = 5$

so $1 + ab = 1 + 2^7 \cdot 5 = 641$

Since $1 + ab - b^4 = 1 + (a - b^3)b = 1 + (128 - 125)b = 1 + 3b = 2^4$

But implies that

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4 (2^7)^4 + 1 = 2^4 a^4 + 1 = (1 + ab - b^4) a^4 + 1 =$

$= (1 + ab) a^4 + (1 - a^4 b^4) = (1 + ab) a^4 + (1 - a^2 b^2)(1 + a^2 b^2) =$

$= (1 + ab) a^4 + (1 - ab)(1 + ab)(1 + a^2 b^2) = (1 + ab)[a^4 + (1 - ab)(1 + a^2 b^2)]$

$= 641 / F_5$, so $F_5$ is composite number.

And the prime factors of number $F_5$ are 641, 6700417

The multiplication of two primes give us the number $F_5$

So using modulo arithmetic we observe:

$P = 641$

$641 \equiv 1 \mod 64$

$6700417 \equiv 1 \mod 64$

## Exercise 9

From the definition An odd ~~integer~~ composite integer $n$ is an Euler pseudoprime to the base $b$ if

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n \quad \text{where } \left(\frac{b}{n}\right) = \pm 1 \text{ is the Jacobi symbol}$$

So, the example $91$ is a pseudoprime to the base $3$ since $3^{90} \equiv 1 \bmod 91$

On the other hand $3^{45} \equiv 27 \bmod 91$ so $91$ is not an Euler pseudoprime to the base $3$.

Exercise 11

We shall show that if $n$ is a pseudoprime to the base 2, then $2^n - 1$ is a strong pseudoprime to the base 2. Let $n$ be an odd which is a pseudoprime to the base 2. Hence, $n$ and $N = 2^n - 1$ are composite, and $2^n - 1 \equiv 1 \bmod n$

From this congruence we can see that $2^{n-1} - 1 \equiv nk$ for some integer $k$

moreover $k$ must be odd, we have $N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk$

this is a factorization of $N-1$ into an odd integer and a power of 2.

Now, $2^{\frac{N-1}{2}} = 2^{nk} = (2^n)^k \equiv 1 \pmod N$, because $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \bmod N$

This implies that $N$ is a strong pseudoprime to the base 2. Since every pseudoprime $2^n - 1$ yields a strong pseudoprime to the base 2 and since there are infinitely many pseudoprimes to the base 2. So, there are exist infinitely many strong pseudoprimes to the base 2

Exercise 14

Applying AKS Algorithm

Input: $n = 16493$ is an odd positive integer

Output: the answer is $n$ composite

Because $n \neq a^b$ for some numbers $a, b$ with $b > 1$ then the output is not composite

Find the smallest prime $p$ with $ord_p(n) > 4(\log_2 n)^2 + 2$ and let

$l = [2\sqrt{r} \log_2 n] + 1$

check if an integer $2, 3, \ldots, l$ divide number $n$ $(2, 3, \ldots, l / n)$

$4(\log_2 n)^2 + 2 = 787.071$

So $p = 797$ and $l = 792$

So $1, \ldots, 792 / 16493$

After we check if $(x-a)^n \not\equiv x^n - a \pmod{x^r - 1} \in \mathbb{Z}_{16493}$ $n = 16493$

for $a \in \{1, \ldots, 792\}$. So the congruence $(x-a)^n \not\equiv x^n - a \pmod{x^r - 1}$

is not true. Hence, the number 16493 is <u>prime</u>

Exercise 13

If $n = p^a$, where $p$ is prime and $a$ integer $> 1$. Prove that $n$ is strong pseudoprime to the base $b$ if and only if $n$ is pseudoprime of Fermat to the base $b$.

Solution

$\Rightarrow$ $n$ is a strong pseudoprime so from the theory we have $\gcd(b,n) = 1$

~~Set~~ $n = 2^s z + 1$ $n$ is ~~a~~ strong pseudoprime in base $b$ $b^t \equiv 1 \bmod n$

where $t = \varphi(n-1)$ So $n$ is a Fermat pseudoprime

$\Leftarrow$ from the definition we can take the result

1) Έστω $x$ θετικός πραγματικός αριθμός που αναπτύσσεται σε συνεχές κλάσμα:

$$x = [a; a, \dots]$$

όπου $a$ θετικός ακέραιος. Ν.δ.ο. ότι ο $x$.

Λύση

Από τη θεωρία

$$x = a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{\ddots}}}}}$$

$a_0 = a$

$a_1 = a$

$a_2 = a$

$\vdots$ } infinite

$$x = a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{y}}} \Leftrightarrow$$

$$x = a + \cfrac{1}{a + \cfrac{1}{\frac{ay+1}{y}}} = a + \cfrac{1}{a + \frac{y}{ay+1}} = a + \cfrac{1}{\frac{a^2y+a+y}{ay+1}} =$$

$$= a + \frac{ay+1}{a^2y+a+y} = \frac{a^3y + a^2 + ay + ay + 1}{a^2y + a + y} = \frac{a^3y + 2ay + 1 + a^2}{a^2y + ay + y}$$

Αντιπρότυπο

2) Να υπολογιστεί το ανάπτυγμα σε συνεχές κλάσμα των ρητών

$$\frac{51}{23} = [2; 4, 1, 1, 2]$$

$$51 = 23 \cdot 2 + 5$$
$$23 = 5 \cdot 4 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

$$[a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

$$\frac{13}{25} = [0; 1, 1, 12]$$

$$13 = 25 \cdot 0 + 13$$
$$25 = 13 \cdot 1 + 12$$
$$13 = 12 \cdot 1 + 1$$
$$12 = 1 \cdot 12 + 0$$

$$\frac{37}{45} = [0; 1, 4, 1, 1, 1, 2]$$

$$37 = 45 \cdot 0 + 37$$
$$45 = 37 \cdot 1 + 8$$
$$37 = 8 \cdot 4 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

- $\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}]$

$\sqrt{19} = \underline{4} + \sqrt{19} - 4$

$\frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} = \underline{2} + \frac{\sqrt{19}-2}{3}$

$\frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5} = \underline{1} + \frac{\sqrt{19}-3}{5}$

$\frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2} = \underline{3} + \frac{\sqrt{19}-3}{2}$

$\frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5} = \underline{1} + \frac{\sqrt{19}-2}{5}$

$\frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3} = \underline{2} + \frac{\sqrt{19}-4}{3}$

$\frac{3}{\sqrt{19}-4} = \sqrt{19}+4 = \underline{8} + (\sqrt{19}-4)$

- $\sqrt{44} = [6; \overline{1, 1, 1, 2, 1, 1, 1, 12}]$

- $\sqrt{\frac{8}{3}} = [1; \overline{1, 1, 1, 2}]$

3)

(a) $\sqrt{n^2+1} = n + \dfrac{\sqrt{n^2+1}-n}{1} = n + \dfrac{1}{\sqrt{n^2+1}+n} = n + \dfrac{1}{2n + \dfrac{\sqrt{n^2+1}-n}{1}} = \dots$

So, $\sqrt{n^2+1} = [n; \overline{2n}]$

(b) $\sqrt{n^2-1} = (n-1) + \sqrt{n^2-1} - (n-1) = (n-1) + \dfrac{1}{\dfrac{1}{\sqrt{n^2-1}-(n-1)}} = (n-1) + \dfrac{1}{\dfrac{\sqrt{n^2-1}+(n-1)}{2(n-1)}} =$

$= (n-1) + \dfrac{1}{1 + \dfrac{\sqrt{n^2-1}-(n-1)}{2n-2}} = (n-1) + \dfrac{1}{1 + \dfrac{1}{\dfrac{2(n-1)}{\sqrt{n^2-1}-(n-1)}}} = (n-1) + \dfrac{1}{1 + \dfrac{1}{\dfrac{2(n-1)(\sqrt{n^2-1}+(n-1))}{2(n-1)}}} =$

$= (n-1) + \dfrac{1}{1 + \dfrac{1}{\sqrt{n^2-1}+(n-1)}}$ So, $\sqrt{n^2-1} = [n-1; \overline{1, 2n-2}]$

(c) $\sqrt{n^2+2} = n + (\sqrt{n^2+2} - n) = n + \dfrac{2}{\sqrt{n^2+2}+n} = +n + \dfrac{1}{\dfrac{2n}{2} + \dfrac{\sqrt{n^2+2}-n}{2}} =$

$= n + \dfrac{1}{\dfrac{2n}{2} + \dfrac{1}{\sqrt{n^2+2}+n}} = n + \dfrac{1}{n + \dfrac{1}{2n + (\sqrt{n^2+2}-n)}}$

Hence, $\sqrt{n^2+2} = [n; \overline{n, 2n}]$

4) $\theta$ irrational number

Since $\theta - \frac{p_n}{q_n}$ and $\theta - \frac{p_{n+1}}{q_{n+1}}$ have positive signs

$$\left|\theta - \frac{p_n}{q_n}\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2}$$

from the last inequality : $ab < \frac{a^2+b^2}{2}$ with $a \neq b$ $a = \frac{1}{q_{n+1}}$ and $b = \frac{1}{q_n}$

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_n^2+1}$$

The above ~~the above theor~~ proposition is the Vahlen's proposition (1895)

5) (Borel, 1903) let $x = \theta$, $\theta$ is a irrational number

for $n \geq 0$, $q_n x - p_n = \dfrac{(-1)^n}{x_{n+1} q_n + q_{n-1}}$

Therefore $|q_n x - p_n| < \dfrac{1}{\sqrt{5}\, q_n}$ if and only if $|x_{n+1} q_n + q_{n-1}| > \sqrt{5}\, q_n$

Define $r_n = \dfrac{q_{n-1}}{q_n}$ $\Longrightarrow$ is equivalent $|x_{n+1} + r_n| > \sqrt{5}$

so, $x_{n+1} = a_{n+1} + \dfrac{1}{x_{n+2}}$

Using the definition for $r_n$ and $r_{n+1}$, $q_{n+1} = a_{n+1} q_n + q_{n-1}$

we ~~ei~~ write $\dfrac{1}{r_{n+1}} = a_{n+1} + r_n$

Eliminate $\dfrac{1}{x_{n+2}} + \dfrac{1}{r_{n+1}} = x_{n+1} + r_n$

Let's assume $|x_{n+1} + r_n| \leq \sqrt{5}$ and $|x_{n+2} + r_{n+1}| \leq \sqrt{5}$

We deduce $\dfrac{1}{\sqrt{5} - r_{n+1}} + \dfrac{1}{r_{n+1}} \leq \dfrac{1}{x_{n+2}} + \dfrac{1}{r_{n+1}} = x_{n+1} + r_n \leq \sqrt{5}$

$$\Longrightarrow r_{n+1}^2 - \sqrt{5}\, r_{n+1} + 1 \leq 0$$

The polynomial $X^2 - \sqrt{5} X + 1$ has roots $\phi = \dfrac{1+\sqrt{5}}{2}$ and $\phi^{-1} = \dfrac{(\sqrt{5}-1)}{2}$

$\left(\phi = \dfrac{1+\sqrt{5}}{2} \text{ is the golden ratio}\right)$, so $r_{n+1} > \phi^{-1}$

From above we have the following result: from hypotheses $|q_n x - p_n| < \dfrac{1}{\sqrt{5}\, q_n}$ and $|q_{n+1} x - p_{n+1}| < \dfrac{1}{\sqrt{5}\, q_{n+1}}$. if also had $|q_{n+2} x - p_{n+2}| < \dfrac{1}{\sqrt{5}\, q_{n+2}}$

with the same way $r_{n+2} > \phi^{-1}$. ~~with~~ which give us $1 = (a_{n+2} + r_{n+1}) r_{n+1} > (1 + \phi^{-1}) \phi^{-1} = 1$

which is impossible.

6) We have $\frac{a}{b} \in \mathbb{Q}$ and let $[a_0; a_1, a_2, \ldots, a_n]$ a continued fraction

we know $\frac{p_n}{q_n} = \frac{a}{b} \Rightarrow p_n b = a q_n$

Now $a \mid p_n b$, $(a,b) = 1 \Rightarrow a \mid p_n$

$b \mid q_n a$, $(a,b) = 1 \Rightarrow b \mid q_n$

Hence, $p_n = \pm a$, $q_n = \pm b$ . where $b > 0$ $q_n > 0 \Rightarrow \begin{cases} q_n = b \\ p_n = a \end{cases}$

So from the relationship we have $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$

$\Rightarrow a q_{n-1} - b p_{n-1} = (-1)^{n-1}$

So, $x = (-1)^n q_{n-1}$ and $y = (-1)^n p_{n-1}$

Άσκηση 7

$x = [1; \overline{1,1,2}]$ και $y = [\overline{1,1,2}]$

$$x = 1 + \frac{1}{y}$$

$$y = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{y}}} = \frac{5y+2}{3y+1} \Leftrightarrow 3y^2 + y = 5y + 2 \Leftrightarrow 3y^2 - 5y + y - 2 = 0 \Leftrightarrow$$

$$3y^2 - 4y - 2 = 0$$

$$y_{1,2} = \frac{2 \pm \sqrt{10}}{3}$$

- $\frac{2y+1}{y}$

$$1 + \frac{1}{\frac{2y+1}{y}} = 1 + \frac{y}{2y+1} = \frac{2y+1+y}{2y+1} = \frac{3y+1}{2y+1}$$

$$1 + \frac{2y+1}{3y+1} = \frac{3y+1+2y+1}{3y+1} = \frac{5y+2}{3y+1}$$

Κρατάμε το θετικό $y = \frac{2+\sqrt{10}}{3}$

$$x = 1 + \frac{1}{\frac{2+\sqrt{10}}{3}} = 1 + \frac{3}{2+\sqrt{10}} = \frac{2+\sqrt{10}+3}{2+\sqrt{10}} = \frac{5+\sqrt{10}}{2+\sqrt{10}}$$

• $x = [\overline{4,1,3}]$

$\alpha_0 = 0$

$$x = 0 + \frac{1}{y} = \frac{1}{\frac{9+\sqrt{101}}{4}} = \frac{4}{9+\sqrt{101}}$$

$$y = 4 + \frac{1}{1+\frac{1}{3+\frac{1}{y}}} \Leftrightarrow y = \frac{19y+5}{4y+1} \Leftrightarrow 4y^2 + y = 19y + 5$$

$$4y^2 - 18y - 5 = 0$$

$$y_{1,2} = \frac{9}{4} \pm \frac{\sqrt{101}}{4} = \frac{9 \pm \sqrt{101}}{4}$$

$$\frac{3y+1}{y} \qquad 1 + \frac{1}{\frac{3y+1}{y}} = 1 + \frac{y}{3y+1} = \frac{3y+1+y}{3y+1} = \frac{4y+1}{3y+1}$$

$$4 + \frac{1}{\frac{4y+1}{3y+1}} = 4 + \frac{3y+1}{4y+1} = \frac{16y+4+3y+1}{4y+1} = \frac{19y+5}{4y+1}$$

Κρατάμε το θετικό $y = \frac{9+\sqrt{101}}{4}$

Άσκηση 7

- $x = [1; 2, 3, \overline{1,4}]$ $\qquad y = [\overline{1,4}]$

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{y}}} \qquad\qquad y = 1 + \cfrac{1}{4 + \cfrac{1}{y}} \; *$$

$$* \quad \frac{1}{\frac{4y+1}{y}} = \frac{y}{4y+1} + 1 = \frac{y+4y+1}{4y+1} = \frac{5y+1}{4y+1}$$

$$y = \frac{5y+1}{4y+1} \Leftrightarrow 4y^2 + y = 5y + 1 \Leftrightarrow$$

$$4y^2 - 4y - 1 = 0$$

$$y_{1,2} = \frac{1 \pm \sqrt{2}}{2}$$ κρατάμε το θετικό

$$y = \frac{1+\sqrt{2}}{2}$$

$$3 + \frac{1}{\frac{1+\sqrt{2}}{2}} = 3 + \frac{2}{1+\sqrt{2}} = \frac{3+3\sqrt{2}+2}{1+\sqrt{2}} = \frac{5+3\sqrt{2}}{1+\sqrt{2}}$$

$$2 + \frac{1}{\frac{5+3\sqrt{2}}{1+\sqrt{2}}} = 2 + \frac{1+\sqrt{2}}{5+3\sqrt{2}} = \frac{10+6\sqrt{2}+1+\sqrt{2}}{5+3\sqrt{2}} = \frac{11+7\sqrt{2}}{5+3\sqrt{2}}$$

$$1 + \frac{5+3\sqrt{2}}{11+7\sqrt{2}} = \frac{11+7\sqrt{2}+5+3\sqrt{2}}{11+7\sqrt{2}} = \frac{16+10\sqrt{2}}{11+7\sqrt{2}}.$$

8)

Θεωρώ πραγματικό αριθμό $\theta = e$. Θέτω $a_0 = \lfloor \theta \rfloor$

$\Rightarrow \lfloor e \rfloor = 2$. Επειδή $\theta = \theta_0 \neq a_0$ τότε $\theta_0 = \theta = a_0 + \frac{1}{\theta_1} \Rightarrow \theta = \frac{1}{\theta - a_0} \Rightarrow$

$\Rightarrow \theta_1 = 1{,}39$

$a_1 = \lfloor \theta_1 \rfloor = 1$. Επειδή $\theta_i \neq a_i$

$$\theta_1 = a_1 + \frac{1}{\theta_2} \Rightarrow \theta_2 = \frac{1}{\theta_1 - a_1} = 2{,}56 \qquad a_2 = \lfloor \theta_2 \rfloor = 2$$

$$\theta_3 = \frac{1}{\theta_2 - a_2} = 1{,}78 \Rightarrow a_3 = \lfloor \theta_3 \rfloor = 1$$

$$\theta_4 = \frac{1}{\theta_3 - a_3} = 1{,}28 \Rightarrow a_4 = \lfloor \theta_4 \rfloor = 1$$

$$\theta_5 = \frac{1}{\theta_4 - a_4} = 3{,}57 \Rightarrow a_5 = \lfloor \theta_5 \rfloor = 3$$

$$\theta_6 = \frac{1}{\theta_5 - a_5} = 1{,}75 \Rightarrow a_6 = \lfloor \theta_6 \rfloor = 1$$

$$\theta_7 = \frac{1}{\theta_6 - a_6} = 1{,}\bar{3} \Rightarrow a_7 = \lfloor \theta_7 \rfloor = 1$$

$\theta_i \neq a_i$

$$\theta_8 = \frac{1}{\theta_7 - a_7} = 3{,}3 \Rightarrow a_8 = \lfloor \theta_8 \rfloor = 3$$

$$\theta_9 = \frac{1}{\theta_8 - a_8} = 3{,}3 \Rightarrow a_9 = \lfloor \theta_9 \rfloor = 3 \quad \text{Άρα } a_{10} = 3$$

Άρα $e = [2; 1, 2, 1, 1, 3, 1, 1, 3, 3]$

Από Dirichlet ξέρουμε ότι υπάρχουν άπειροι ρητοί αριθμοί $\frac{p}{q}$ τέτοιοι $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{Q^2}$

$\theta = e$ $\quad \left|\theta = e - \frac{P_k}{Q_k}\right| \leq \frac{1}{2} \frac{1}{Q_k^2}$

9) Find the period of continued fraction of $\sqrt{13290059}$

<u>Solution</u>

$$\sqrt{13290059} = [3645; 1, 1, 4, 5, 3, 2, 1, 2, 1, 4, 1, 2, 1, 5, 1, 1, 3, 2, 5, 1, 1, 1, 34, \ldots]$$

So, the lenght of periodic part of continued fraction is <u>1068</u>

## ΦΡΟΝΤΙΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ

**επί της 6ης Ενότητας (Μέρος Πρώτο)**

**"ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΑΚΕΡΑΙΩΝ"**

**Ασκηση 1.**
Να χρησιμοποιηθεί η μέθοδος του Fermat για να παραγοντοποιηθούν οι ακέραιοι

$$\underbrace{4601}_{e},\ \underbrace{8633}_{a},\ 13199,\ \underbrace{809009}_{b}.$$

**Ασκηση 2.**
Να χρησιμοποιηθεί η γενίκευση της μεθόδου του Fermat για να παραγοντοποιηθούν οι αριθμοί

$$141467 \text{ και } 68987.$$

**Ασκηση 3.**
Έστω $n = 4633$. Να βρεθεί η μικρότερη βάση παραγοντοποίησης $B$ η οποία είναι τέτοια, ώστε οι αριθμοί $68$, $69$ και $96$ να είναι $B$ −προσαρμοσμένοι ως προς $n$ και με την βοήθεια της $B$ να παραγοντοποιηθεί ο αριθμός $4633$.

**Ασκηση 4.**
Να χρησιμοποιηθεί ο αλγόριθμος του Dixon για να παραγοντοποιηθούν οι ακέραιοι

$$256961 \text{ και } 1829.$$

**Ασκηση 5.**
Να χρησιμοποιηθεί η μέθοδος των συνεχών κλασμάτων για την παραγοντοποίηση των ακεραίων

$$\underset{k}{17873},\ \underset{b}{13561} \text{ και } \underset{j}{25511}.$$

**Ασκηση 6.**
Να χρησιμοποιηθεί ο αλγόριθμος $p - 1$ του Pollard για την παραγοντοποίηση των ακεραίων

$$16867 \text{ και } 29651.$$

101 167

**Ασκηση 7.**
Να χρησιμοποιηθεί ο αλγόριθμος $\rho$ του Pollard για την παραγοντοποίηση των ακεραίων

$$5141,\ 262063 \text{ και } 25279.$$

**Ασκηση 8.**
Ας υποθέσουμε ότι $m$, $n$, $a$, $b$ και $c$ είναι θετικοί ακέραιοι:

(α) Αν $m|(b^a - 1)$, $m|(b^c - 1)$ και $d = gcd(a, c)$, τότε να δειχθεί ότι $m|(b^d - 1)$.

(β) Αν $p$ είναι ένας πρώτος διαιρέτης του $b^n - 1$, τότε να δειχθεί ότι $p|(b^\delta - 1)$ για κάποιο θετικό διαιρέτη $\delta$ του $n$ με $\delta < n$ ή $p \equiv 1\ (mod\ n)$. Ιδιαιτέρως, εάν $p > 2$ και ο $n$ είναι περιττός, τότε στη δεύτερη περίπτωση ισχύει $p \equiv 1\ (mod\ 2n)$.

(γ) Να χρησιμοποιηθεί το παραπάνω αποτέλεσμα για την παραγοντοποίηση των ακεραίων

$$2^{11} - 1 \text{ και } 3^{12} - 1.$$

**Ασκηση 9.**
Ας είναι $b$ και $m$ ακέραιοι $\geq 2$. Ένας πρώτος $p > 2$ είναι παράγοντας του $b^m + 1$ αν και μόνον αν είναι παράγοντας του $b^{2m} + 1$.

1) $n = 4601$

$\lfloor\sqrt{4601}\rfloor = 67$, $t = \lfloor\sqrt{4601}\rfloor + 8 = 67 + 8 = 75$

$t^2 - n = s^2 \Leftrightarrow t^2 - n = 5625 - 4601 = 1024 \Rightarrow s = 32$

So, $s^2 = 1024$ is a perfect square.

Hence, $75^2 - 4601 = 32^2$

$\Rightarrow 4601 = 75^2 - 32^2 = (75-32)(75+32) = 43 \cdot 107$

$\boxed{4601 = 43 \cdot 107}$

$n = 8633$

$\lfloor\sqrt{8633}\rfloor = 92$ $t = \lfloor\sqrt{8633}\rfloor + 1 = 92 + 1 = 93$

$t^2 - n = s^2 \Leftrightarrow t^2 - n = 8649 - 8633 = 16 \Rightarrow s^2 = 16 \Rightarrow s = 4$

$s^2 = 16$ is a perfect square.

Hence, $8649 - 8633 = 16 \Leftrightarrow$

$8633 = 8649 - 16 = 93^2 - 16 = (93-4)(93+4) =$

$= 89 \cdot 97$

So, the prime factors of $\boxed{8633 = 89 \cdot 97}$

$n = 809009$

$\lfloor\sqrt{809009}\rfloor = 899$ $t = \lfloor\sqrt{809009}\rfloor + 4 = 903$

$t^2 - n = s^2 \Leftrightarrow t^2 - n = 903^2 - 809009 = 6400 \Rightarrow s = 80$

Hence, $n = t^2 - s^2 = (t-s)(t+s) = (903-80)(903+80) =$

$= 823 \cdot 983$

$\boxed{809009 = 823 \cdot 983}$

$n = 13199$

$\lfloor \sqrt{13199} \rfloor = 114 \qquad t = \lfloor \sqrt{13199} \rfloor + 2074 = 2188$

So, $t^2 = 4787344$

$t^2 - n = \cancel{16162 - 13119 = 1042 \Rightarrow s = \sqrt{1042} = 32}$

~~Hence~~ $\cancel{n = t^2 - s^2 = (t-s)(t+s) = (\sqrt{1042} - 32)(\sqrt{1042} + 32)}$

$= \cancel{(119-32)(119+32) = 87 \cdot 151}$

$t^2 - n = 4787344 - 13199 = 4774225 \Rightarrow s = \cancel{2188}\ 2185$

$t^2 - n = s^2 \Leftrightarrow n = (t-s)(t+s) = (2188 - 2185)(2188 + 2185) =$

$= 3 \cdot 4373$

Hence, $\boxed{13199 = 3 \cdot 4373}$

3) 2) Using generalized Fermat factorization:

$n = 68987$

$$\lfloor \sqrt{3 \cdot n} \rfloor = \lfloor \sqrt{206961} \rfloor = 454$$

$$t = \lfloor \sqrt{3 \cdot n} \rfloor + 1 = 454 + 1 = 455$$

$$t^2 - kn = s^2 \Rightarrow 455^2 - 3 \cdot n = 207025 - 206961 = 64$$

$$\Rightarrow s^2 = 64 \Rightarrow \underline{s = 8}$$

$$\Rightarrow kn = t^2 - s^2 \Leftrightarrow$$

$$kn = (t-s)(t+s) \Leftrightarrow$$

$$3n = (t-s)(t+s) = (455-8)(455+8) = 447 \cdot 463$$

$$\gcd(68987, 463) = 463$$

Hence, $\boxed{68987 = 463 \cdot 149}$

$n = 141467$

$$\lfloor \sqrt{3 \cdot n} \rfloor = \lfloor \sqrt{424401} \rfloor = 651$$

$$t = \lfloor \sqrt{3 \cdot n} \rfloor + 4 = 651 + 4 = 655$$

$$t^2 - kn = s^2 \Leftrightarrow$$

$$655^2 - 3 \cdot (141467) = 429025 - 424401 = \underset{s^2}{\underset{\parallel}{4624}} \Rightarrow \boxed{s = 68}$$

$$kn = t^2 - s^2 = (t-s)(t+s) = (655-68)(655+68) =$$

$$= 587 \quad 723$$

$$\gcd(141467, 723) = 241$$

Hence, $\boxed{141467 = 241 \cdot 587}$

3) As we saw, $68^2 \bmod n$ and $69^2 \bmod n$ are products of $-1$, 2 and 3. Since $96^2 \bmod n = -50$, the least absolute residues of all three squares can be written in terms of the factor-base $B = \{-1, 2, 3, 5\}$. We have compute the vectors $\vec{e}_1 = (1, 0, 0, 0)$ and $\vec{e}_2 = (0, 1, 0, 0)$ corresponding to 68 and 69, respectively. Since, $96^2 \equiv -50 \bmod 4633$ we have $\vec{e}_3 = (1, 1, 0, 0)$. Since the sum of these vectors is zero ($\mathbb{Z}_2$) we can take $b = 68 \cdot 69 \cdot 96 = 1031 \bmod 4633$ and $c = 2^4 \cdot 3 \cdot 5 = 240$. Then, we obtain $\gcd(240 + 1031, 4633) = 41$.

4) for $N = 1829$ applying the Pixon's Algorithm $B = 13$

We take the base $B = \{-1, 2, 3, 5, 7, 11, 13\}$

We select simply a random $r$ and check whether $r^2 \bmod N$ is B-smooth

We select the values $\lfloor \sqrt{kN} \rfloor$ and $\lceil \sqrt{kN} \rceil$ for $k = 1, 2, 3, 4$ and test whether square of each modulo 1829 is B-smooth:

$42^2 = 1764 = -65 = -1 \cdot 5 \cdot 13 \mod 1829$

$43^2 = 20 = 2^2 \cdot 5 \mod 1829$

$60^2 = 1771 = -58 = -1 \cdot 2 \cdot 29 \mod 1829$

$61^2 = 63 = 3^2 \cdot 7 \mod 1829$

$74^2 = 1818 = -11 = -1 \cdot 11 \mod 1829$

$75^2 = 138 = 2 \cdot 3 \cdot 23 \mod 1829$

$85^2 = 1738 = -91 = -1 \cdot 7 \mod 1829$

$86^2 = 80 = 2^4 \cdot 5 \mod 1829$

All of these are B-smooth except $60^2$ and $75^2$, give us useful relations

Now, for each of the six B-smooth values we obtain a mode vector of length seven

$42^2 = -65 \rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$ $43^2 = 20 \rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ $61^2 = 63 \rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ $74^2 = -11 \rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$

$85^2 = -91 \rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$ $86^2 = 80 \rightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

We sum the vectors of $42^2, 43^2, 61^2$ and $85^2$

$$\begin{bmatrix}1\\0\\0\\1\\0\\0\\1\end{bmatrix} \oplus \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\end{bmatrix} \oplus \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\end{bmatrix} \oplus \begin{bmatrix}1\\0\\0\\0\\1\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\end{bmatrix}$$

$42^2 \cdot 43^2 \cdot 61^2 \cdot 85^2 \equiv (-65) \cdot 20 \cdot 63 \cdot (-91) = (-1 \cdot 5 \cdot 13) \cdot (2^2 \cdot 5)(3^2 \cdot 7)(-1 \cdot 7 \cdot 13) =$

$= 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \bmod 1829 \Longleftrightarrow$

$(42 \cdot 43 \cdot 61 \cdot 85)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2 \bmod 1829$

So, simply if we do the multiplication we can see,

$1459^2 \equiv 901^2 \bmod 1829$

Since $1459 - 901 = 558$

$\gcd(1829, 558) = 31$

Now it's easy to observe that $1829 = 59 \cdot 31$

4) for $N = 256961$ and $B = 31$ $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$

$k = 1, 2, 3, 4$

$\lfloor \sqrt{1 \cdot N} \rfloor = \lfloor \sqrt{256961} \rfloor = 506$ $\qquad 506^2 = 256036 = 2^2 \cdot 11^2 \cdot 23^2 \bmod 256961$

$\lceil \sqrt{N} \rceil = 507$ $\qquad -507^2 = 88 = 2^3 \cdot 11 \bmod 256961$

$\lfloor \sqrt{2N} \rfloor = \lfloor \sqrt{513922} \rfloor = 716$ $\qquad 716^2 = 255695 = 5 \cdot 11 \cdot 4649 \bmod N$

$\lceil \sqrt{2N} \rceil = 717$ $\qquad 717^2 = 167 \bmod N$

$\lfloor \sqrt{3N} \rfloor = \lfloor \sqrt{770883} \rfloor = 877$ $\qquad 877^2 = 255207 = 3 \cdot 97 \cdot 877 \bmod N$

$\lceil \sqrt{3N} \rceil = \lceil \sqrt{770883} \rceil = 878$ $\qquad 878^2 = 1 \bmod N$

$\lfloor \sqrt{4N} \rfloor = \lfloor \sqrt{1027844} \rfloor = 1013$ $\qquad 1013^2 = 2 \cdot 127643 \bmod N$

$\lceil \sqrt{4N} \rceil = 1014$ $\qquad -1014^2 = 352 = 2^5 \cdot 11 \bmod N$

$(506 \cdot 507 \cdot 1014)^2 = 2^2 \cdot 11^2 \cdot 23^2 \cdot 2^3 \cdot 11 \cdot 2^5 \cdot 11 \bmod N \Leftrightarrow$

$154528 - 176 = 154352$

$\gcd(154352, N) = 877$

$(878 \cdot 507 \cdot 1014)^2 = 2^8 \cdot 11^2 \cdot 1 \bmod N$

$(154528) = (176)^2 \bmod N$

So, after a few am Euclidean divise we find

$256961 = 877 \cdot 293$

4 iii)

5) Using the method of continued fractions

17873

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | 133 | 1 | 2 | 3 | 2 | 3 | 1 | 2 | 1 |
| $b_i$ | 133 | 134 | 401 | 1738 | 3877 | 13365 | 17246 | 12115 | 11488 |
| $b_i^2 \bmod n$ | -184 | 83 | -56 | 107 | -64 | 161 | -77 | 149 | -88 |

$B = \{-1, 2, 7, 11, 23\}$, $b = 401 \cdot 3877 \cdot 17246 \cdot 11488$

$c = 2^6 \cdot 7 \cdot 11$

$\gcd(b+c, n) = 61$

$\boxed{17873 = 61 \cdot 293}$

13561

| $i$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a_i$ | 116 | 2 | 4 | 1 |
| $b_i$ | 116 | 233 | 1048 | 1281 |
| $b_i^2 \bmod n$ | -105 | 45 | -137 | 80 |

$B = \{2, 3, 5\}$, $b = 233 \cdot 1281$, $c = 2^2 \cdot 3 \cdot 5$, $\gcd(b+c, n) = 191$

$\boxed{13561 = 191 \cdot 71}$

25511

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | 159 | 1 | 2 | 1 | 1 | 2 | 4 | 1 | 5 | 1 |
| $b_i$ | 159 | 160 | 479 | 639 | 1118 | 2875 | 12618 | 15493 | 13550 | 3532 |
| $b_i^2 \bmod n$ | -230 | 89 | -158 | 145 | -115 | 61 | -227 | 50 | -167 | 145 |

$B = \{-1, 2, 5, 23, 29\}$ $b = 639 \cdot 3532$ $c = 5 \cdot 29$ $\gcd(b+c, n) = 97$

$\boxed{25511 = 97 \cdot 263}$

6)

Using P-1 Pollard

for $n = 16867$

$a = 2^2 \bmod 16867 = 4$

$d = \gcd(3, 16867) = 1$

$j = 2+1 = 3$

$a = 4^3 \bmod 16867 = 64$

$d = \gcd(63, 16867) = 1$

$j = 3+1 = 4$

$a = 64^4 \bmod 16867 = 11418$

$d = \gcd(11417, 16867) = 1$

$j = 4+1 = 5$

$a = 11418^5 \bmod 16867 = 3731$

$d = \gcd(3730, 16867) = 1$

$j = 5+1 = 6$

$a = 3731^6 \bmod n = 4993$

$d = \gcd(4992, n) = 1$

$j = 6+1 = 7$

$a = 4993^7 \bmod n = 11954$

$d = \gcd(11953, n) = 1$

$j = 7+1 = 8$

$a = 11954^8 \bmod n = 13124$

$d = \gcd(13123, n) = 1$

$j = 8+1 = 9$

$a = 13124^9 \bmod n = 8366$

$d = \gcd(8365, n) = 1$

$j = 9+1 = 10$

$a = 8366^{10} \bmod n = 2627$

$d = \gcd(2626, n) = 101$ Hence; $\boxed{16867 = 101 \cdot 167}$

**P-1 Pollard**

Input: $n$ to be factored and a bound $B$

Output: $d$, a non-trivial factor of $N$ or failure

```
a ← 2
j ← 2
While j ≤ B do
    a ← a^j mod n
    d ← gcd(a-1, n)
    if 1 < d < N then
        return d
    end if
    j ← j+1
end while
return failure
```

Now if $n =$ 29651 <u>Using P-1 Pollard</u>

$a = 2^2 \bmod n = 4$

$d = \gcd(3, n) = 1$

$j = 2+1 = 3$

$a = 4^3 \bmod n = 64$

$d = \gcd(63, n) = 1$

$j = 3+1 = 4$

$a = 64^4 \bmod n = 24401$

$d = \gcd(24400, n) = 1$

$j = 4+1 = 5$

$a = 24401^5 \bmod n = 22975$

$d = \gcd(22974, n) = 1$

$j = 5+1 = 6$

$a = 22975^6 \bmod n = 20685$

$d = \gcd(20684, n) = 1$

$j = 6+1 = 7$

$a = 20685^7 \bmod n = 2491$

$d = \gcd(2490, n) = 1$

$j = 7+1 = 8$

$a = 2491^8 \bmod n = 8148$

$d = \gcd(8147, n) = 1$

$j = 8+1 = 9$

$a = 8148^9 \bmod n = 3309$

$d = \gcd(3308, n) = 1$

$j = 9+1 = 10$

$a = 3309^{10} \bmod n = 16439$

$d = \gcd(16438, n) = 1$

$j = 10+1 = 11$

$a = 16439^{11} \bmod n = 14727$

$\gcd(14726, n) = 199$

Hence, $\boxed{29651 = 199 \cdot 149}$

7) Using Rho Pollard

$n = 5141$

Let $f(x) = x^2+1$ our seed is $x_0 = 3$, $x_1 = 10$, $x_2 = 101$, $x_3 = 5061$, $x_4 = 1260$

So $\gcd(x_2 - x_0, n) = \gcd(101-3, 5141) = \gcd(97, 5141) = 97$

so, $\boxed{5141 = 97 \cdot 53}$

$n = 262063$

Let $f(x) = x^2+1$ the seed is $x_{35} = 225384$ and $x_{70} = 94604$

Hence, $\gcd(x_{35} - x_{70}, n) = \gcd(130780, n) = 503$

Finally, $\boxed{262063 = 503 \cdot 521}$

$n = 25279$

Let the polynomial $f(x) = x^2+1$

Seed $x_0 = 1$

$x_1 = 2$, $x_2 = 5$, $x_3 = 26$, $x_4 = 677$

$x_5 = 3308$, $x_6 = 22337$, $x_7 = 9947$, $x_8 = 804$, $x_9 = 14442$

$x_{10} = 19615$, $x_{11} = 1846$, $x_{12} = 20331$

So, $\gcd(x_6 - x_{12}, n) = \gcd(22337 - 20331, n) = 17$

Finally $\boxed{25279 = 17 \cdot 1487}$

**Pollard's Rho method**

Steps

(1) Choose an intergal polynomial $f$ with $\deg f \geq 2$
- usually $f(x) = x^2+1$ is chosen for simplicity

(2) Choose a randomly integer $\alpha = x_0$, the seed and compute $x_1 = f(x_0)$, $x_2 = f(x_1)$, ..., $x_{j+1} = f(x_j)$ for $j = 0, 1, 2, \ldots, B$ where the bound $B$ is determined by step (3)

(3) Sieve through all differences $x_i - x_j$ modulo $n$ until it is determined that

$$x_B \not\equiv x_j \bmod n$$

but $x_B \equiv x_j \bmod p$ for some natural number $B > j \geq 1$ Then:

$\gcd(x_B - x_j, n)$ is a nontrivial divisor of $n$.

9) Suppose $p$ is a primitive factor of $b^m+1$. Clearly $p \mid (b^{2m}-1)$ since $(b^m+1) \mid (b^{2m}-1)$. Suppose $p \mid b^k-1$ for some $0<k<2m$. Then $p \mid (b^m+1+b^k-1)$ so $p \mid (b^m+b^k)$. of course $p \nmid b$. If $k<m \Rightarrow p \mid b^k(b^{m-k}+1)$, so $p \mid (b^{m-k}+1)$ and $0<m-k<m$ so $p$ is not a primitive factor of $b^m+1$. If $k>m \Rightarrow p \mid b^m(b^{k-m}+1)$

so $p \mid (b^{k-m}+1)$ and $0<k-m<m$ so $p$ is primitive factor of $b^m+1$

Finally, if $k=m$, then $p \mid 2b^m$, which is impossible because $p$ is odd and $p \nmid b$

Now suppose $p$ is primitive factor of $b^{2m}-1 = (b^m-1)(b^m+1)$. Since $p$ doesn't divide $b^m-1$, it must divide $b^m+1$. if $p$ divided $b^k+1$ for some $0<k<m \rightarrow$ it would divide $b^{2k}-1$. But $0<2k<2m$ so it would not be a primitive factor of $b^{2m}-1$.

## 8.6 Ασκήσεις

1. Να χρησιμοποιηθεί ο αλγόριθμος του Shanks για τον υπολογισμό του διακριτού λογάριθμου του 23 ως προς βάση $g$ μέσα στην ομάδα $\mathbb{Z}_{211}^*$, όπου $g$ είναι η μικρότερη αρχική ρίζα κατά μέτρο 211. $\log_g 23$

2. Ο ακέραιος 347 είναι πρώτος και $173|346$. Να βρεθεί ο μικρότερος γεννήτορας $g$ της μοναδικής κυκλικής υποομάδας $G$ της $\mathbb{Z}_{347}^*$ τάξης 173. Να δειχθεί ότι ο ακέραιος 243 ανήκει στη $G$ και να υπολογιστεί ο διακριτός λογάριθμος $\log_g 243$.

3. Να χρησιμοποιηθεί ο αλγόριθμος του Pollard για τον υπολογισμό του διακριτού λογάριθμου του 507 ως προς βάση 5 μέσα στην ομάδα $\mathbb{Z}_{647}^*$.

4. Να δειχθεί ότι ο 3 είναι η μικρότερη αρχική ρίζα κατά μέτρο 449 και να υπολογιστεί ο διακριτός λογάριθμος της κλάσης 13 ως προς βάση 3 μέσα στην ομάδα $\mathbb{Z}_{449}^*$ με την μέθοδο του λογισμού δεικτών.

5. Ας είναι $p$ πρώτος, $q$ ένας πρώτος με $q|p-1$, $\gamma \in \mathbb{Z}_p^*$ ένα στοιχείο που παράγει την μοναδική ομάδα $G$ τάξης $q$ και $\alpha \in G$. Για $\delta \in G$,

καλούμε *αναπαράσταση του $\delta$ ως προς τα $\gamma$ και $\alpha$*, ένα ζεύγος ακεραίων $(r, s)$ με $0 \leq r, s < q$ με $\delta = \gamma^r \alpha^s$. Να δειχθούν τα εξής:
(α) Για κάθε $\delta \in G$, υπάρχουν ακριβώς $q$ αναπαραστάσεις $(r, s)$ του $\delta$ ως προς τα $\gamma$ και $\alpha$ και μεταξύ αυτών υπάρχει μία ακριβώς με $s = 0$.
(β) Αν είναι γνωστή μία αναπαράσταση $(r, s)$ του 1, με $s \neq 0$, ως προς τα $\gamma$ και $\alpha$, τότε ο διακριτός λογάριθμος $\log_\gamma \alpha$ υπολογίζεται σε πολυωνυμικό χρόνο.
(γ) Δοθέντος $\delta \in G$, μαζί με δύο διακεκριμμένες αναπαραστάσεις του $\delta$ ως προς τα $\gamma$ και $\alpha$, τότε ο διακριτός λογάριθμος $\log_\gamma \alpha$ υπολογίζεται σε πολυωνυμικό χρόνο.

6. Ας είναι $n = pq$, όπου $p$ και $q$ είναι δύο περιττοί πρώτοι με $p \neq q$. Θέτουμε $\lambda = \epsilon\kappa\pi(p-1, q-1)$. Υποθέτουμε ότι διαθέτουμε έναν αλγόριθμο ο οποίος δέχεται ως είσοδο ακεραίους $a$ και $b$ με $a^x \equiv b \pmod{n}$, όπου $x$ θετικός ακέραιος, και υπολογίζει τον $x$.
(α) Να δειχθεί ότι το σύνολο

$$K = \{z \in \mathbb{Z}_n^* / \ z^{\lambda/2} \equiv \pm 1 \mod n\}$$

είναι γνήσια υποομάδα του $\mathbb{Z}_n^*$.
(β) Ας είναι $a \in \mathbb{Z}_n^* \setminus K$ και $x = \mathrm{ord}_n(a)$. Να δειχθεί ότι υπάρχει ακέραιος $k$ με $1 \leq k < \log_2 x$ έτσι, ώστε να ισχύει $a^{x/2^k} \not\equiv \pm 1 \pmod{n}$ και $(a^{x/2^k})^2 \equiv 1 \pmod{n}$.
(γ) Να δειχθεί ότι ο ακέραιος $\mu\kappa\delta(a^{x/2^k} + 1, n)$ είναι $\neq 1, n$ και επομένως ένας μη τετριμμένος διαιρέτης του $n$.

7. Ας είναι $p$ πρώτος, $a$ μία πρωτογενής ρίζα κατά μέτρο $p$ και $x$ θετικός ακέραιος. Αν ο ακέραιος $y = a^x \mod p$ είναι γνωστός, τότε να δειχθεί ότι είναι δυνατόν να συμπεράνουμε σε πολυωνυμικό χρόνο, αν ο $x$ είναι άρτιος ή περιττός.

8. Ας είναι $n$ θετικός ακέραιος. Να δειχθούν τα εξής:
(α) Ο ακέραιος 2 είναι πρωτογενής ρίζα κατά μέτρο $3^n$.
(β) Για κάθε $a \in \mathbb{Z}_{3^n}^*$, το πρόβλημα της εύρεσης του λογαρίθμου $\log_2 a$ μέσα στην ομάδα $\mathbb{Z}_{3^n}^*$ είναι ισοδύναμο με την επίλυση της

$$4^x c \equiv 1 \pmod{3^n},$$

όπου $c \in \mathbb{Z}_{3^n}^*$ και $c \equiv 1 \pmod{3}$.
(γ) Να βρεθεί ένας αλγόριθμος επίλυσης της παραπάνω ισοτιμίας και να υπολογιστεί ο χρόνος εκτέλεσής του.

1) $\log_2 23$ in $\mathbb{Z}^*_{211}$

$n = |\mathbb{Z}^*_{211}| = 210$ $\qquad a = 23$, $g = 2$

$m = \lfloor \sqrt{n} \rfloor + 1 = \lfloor \sqrt{210} \rfloor + 1 = 14 + 1 = 15$

$B = \{ (a g^{-r}, r) : 0 \le r \le m-1 \} =$

$= \{ (23 \cdot 2^{-r}, r) : 0 \le r \le 14 \}$

$(2^{-r} \cdot 23 \bmod 211, r)$

$r=0$ $\quad (23, 0)$

$r=1$ $\quad (2^{-1} \cdot 23, 1) = (117, 1)$

$r=2$ $\quad (2^{-2} \cdot 23, 2) = (164, 2)$

$r=3$ $\quad (2^{-3} \cdot 23, 3) = (82, 3)$

$r=4$ $\quad (2^{-4} \cdot 23, 4) = (41, 4)$

$r=5$ $\quad (2^{-5} \cdot 23, 5) = (126, 5)$

$r=6$ $\quad (2^{-6} \cdot 23, 6) = (63, 6)$

$r=7$ $\quad (2^{-7} \cdot 23, 7) = (137, 7)$

$r=8$ $\quad (2^{-8} \cdot 23, 8) = (179, 8)$

$r=9$ $\quad (2^{-9} \cdot 23, 9) = (87, 9)$

$r=10$ $\quad (2^{-10} \cdot 23, 10) = (149, 10)$

$r=11$ $\quad (2^{-11} \cdot 23, 11) = (180, 11)$

$r=12$ $\quad (2^{-12} \cdot 23, 12) = (90, 12)$

$r=13$ $\quad (2^{-13} \cdot 23, 13) = (45, 13)$

$r=14$ $\quad (2^{-14} \cdot 23, 14) = (128, 14)$

$X = 1 \cdot 15 + 10 = 25$

$\boxed{\log_2 23 = 15 \cdot 1 + 10 = 25}$

$d = 2^{11} \bmod 211 = 149$

$q = 1, 2, \ldots$

$d^q$

$149^1 \bmod 211 \equiv 149$

$149^2 \bmod 211 = 46$

$149^3 \bmod 211 = 102$

$149^4 \bmod 211 = 6$

$149^5 \bmod 211 = 50$

$149^6 \bmod 211 = 65$

$149^7 \bmod 211 = 104$

$149^8 \bmod 211 = 36$

$149^9 \bmod 211 \equiv 89$

$149^{10} \bmod 211 = 179$

$149^{11} \bmod 211 = 85$

$149^{12} \bmod 211 = 5$

$149^{12} \bmod 211 = 112$

3) Calculate $\log_5 507 = ?$ in group $\mathbb{Z}^*_{647}$

<u>Solution</u>

The number 647 is a prime number the $\varphi$-Euler is $\varphi(647) = 646$

The factors of 646 are $2 \cdot 17 \cdot 19$

So the order of $ord_{647}\, 5 = 646$, because $5^{646} \equiv 1 \mod 647$

So the possiblies $ord_{647}\, 5 \in \{2, 17, 19, 34, 38, 323, 646\}$

Now let H subgroup of $\mathbb{Z}^*_{647}$

let a map $f: H \times \mathbb{Z}_{646} \times \mathbb{Z}_{646} \longrightarrow H \times \mathbb{Z}_{646} \times \mathbb{Z}_{646}$

$$f(x,a,b) = \begin{cases} 507\, x \bmod 647,\ a,\ b+1 \bmod 646, & x \in S_1 \quad (1) \\ x^2 \bmod 647,\ 2a \bmod 646,\ 2b \bmod 646, & x \in S_2 \quad (0) \\ 5\, x \bmod 647,\ a+1 \bmod 646,\ b, & x \in S_3 \quad (2) \end{cases}$$

$S_1 = \{x \in \mathbb{Z}^*_{647} : x = 3k+1\}$

$S_2 = \{x \in \mathbb{Z}^*_{647} : x = 3k\}$

$S_3 = \{x \in \mathbb{Z}^*_{647} : x = 3k+2\}$.

We make the table $i(1,0,0)$

| $i$ | $(x_i, a_i, b_i)$ | $(x_{2i}, a_{2i}, b_{2i})$ |
|---|---|---|
| 1 | (507, 0, 1) | (190, 0, 2) |
| 2 | (190, 0, 2) | (515, 0, 4) |
| 3 | (574, 0, 3) | (526, 1, 5) |
| 4 | (515, 0, 4) | |
| 5 | (634, 1, 4) | |
| 6 | (526, 1, 5) | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Continued in the next page.

| | $(x_i, a_i, b_i)$ | $(x_{2i}, a_{2i}, b_{2i})$ |
|---|---|---|
| 1 | (507, 0, 1) | (190, 0, 2) |
| 2 | (190, 0, 2) | (515, 0, 4) |
| 3 | (574, 0, 3) | (526, 1, 5) |
| 4 | (515, 0, 4) | (302, 1, 7) |
| 5 | (634, 1, 4) | (72, 4, 14) |
| 6 | (526, 1, 5) | (40, 9, 28) |
| 7 | (118, 1, 6) | (483, 9, 30) |
| 8 | (302, 1, 7) | (291, 36, 120) |
| 9 | (216, 2, 7) | (288, 72, 241) |
| 10 | (72, 4, 14) | (640, 145, 482) |
| 11 | (8, 8, 28) | (252, 290, 320) |
| 12 | (40, 9, 28) | (490, 581, 640) |
| 13 | (223, 9, 29) | (557, 582, 641) |
| 14 | (483, 9, 30) | (338, 584, 641) |
| 15 | (369, 18, 60) | (242, 524, 636) |
| 16 | (291, 36, 120) | (227, 526, 636) |
| 17 | (571, 72, 240) | (499, 528, 636) |
| 18 | (288, 72, 241) | (348, 528, 638) |
| 19 | (128, 144, 482) | (75, 410, 631) |
| 20 | (640, 145, 482) | (304, 175, 616) |
| 21 | (333, 145, 483) | (177, 175, 618) |
| 22 | (252, 290, 320) | (124, 54, 534) |
| 23 | ~~(98, 580, 640)~~ | ~~(268, 54, 536)~~ |
| 24 | (490, 581, 640) | (36, 108, 428) |
| 25 | (629, 581, 641) | (10, 217, 210) |
| 26 | (557, 582, 641) | (606, 217, 212) |
| 27 | (197, 583, 641) | (312, 222, 202) |
| 28 | (338, 584, 641) | (385, 242, 162) |
| 29 | (396, 585, 641) | (39, 242, 164) |
| 30 | (242, 524, 636) | (488, 485, 328) |
| 31 | (563, 525, 636) | (16, 486, 329) |
| 32 | (227, 526, 636) | (115, 326, 14) |
| 33 | (488, 527, 636) | (449, 6, 30) |
| 34 | (499, 528, 636) | (142, 7, 31) |
| 35 | (16, 528, 637) | (273, 14, 64) |
| 36 | (348, 528, 638) | (109, 28, 129) |
| 37 | (115, 410, 630) | (6, 28, 131) |
| 38 | (75, 410, 631) | (2, 112, 524) |
| 39 | (449, 174, 616) | (541, 113, 525) |
| 40 | (304, 175, 616) | (387, 226, 406) |
| 41 | (142, 175, 617) | (294, 258, 332) |
| 42 | (177, 175, 618) | (448, 516, 19) |
| 43 | (273, 350, 530) | (227, 386, 40) |
| 44 | (124, 54, 534) | (499, 388, 40) |
| 45 | (109, 54, 534) | (348, 388, 42) |
| 46 | (268, 54, 536) | (75, 130, 85) |
| 47 | (6, 54, 537) | (304, 261, 170) |
| 48 | (36, 108, 428) | (177, 261, 172) |
| 49 | (2, 216, 210) | (124, 398, 42) |
| 50 | (10, 217, 210) | (268, 398, 44) |
| 51 | (541, 217, 211) | (36, 150, 90) |
| 52 | (606, 217, 212) | (10, 301, 182) |
| 53 | (387, 434, 424) | (606, 301, 182) |
| 54 | (312, 222, 202) | (312, 558, 82) |
| | $x_i, a_i, b_i$ | $x_{2i}, a_{2i}, b_{2i}$ |

Hence from the algorithm we know:

$$(b_{2i} - b_i) Z \equiv (a_i - a_{2i}) \bmod n$$

So $X_{54} = X_{108} = 312$

$$(82 - 202) Z \equiv 222 - 558 \bmod 646 \Leftrightarrow$$

$$\cancel{-}120 Z \equiv \cancel{-}336 \bmod 646 \Leftrightarrow$$

$$120 Z \equiv 336 \bmod 646$$

$d = \gcd(120, 646) = 2$ $\quad \underline{d \mid 336}$

So the congruence has exactly 2 solutions

$$\frac{120}{2} Z \equiv \frac{336}{2} \bmod \left(\frac{646}{2}\right)$$

$$60 Z \equiv 168 \bmod 323$$

So, $Z = 132 + 323 \cdot k$, $k = 0, 1$

$$\underline{\underline{Z}} = 132, 455$$

So $\log_5 507 = Z$

4) Let $B=13$ so $F(B)=\{2,3,5,7,11,13\}$ so $\log_3 13$

$P=449$ prime

$\phi(449)=449-1=448$

$a^{448}\equiv 1 \bmod 449$

for $a=3$ $3^{448}\equiv 1 \bmod 449$

if exist an $k\in\mathbb{N}$ such that $3^k\equiv 1 \bmod 449$ and $k=ord_{449}(3)$ then $k/448 \Rightarrow k=2,7$

$3^2\equiv 9 \bmod 449$ ✗ (No)

$3^7\equiv 391 \bmod 449$ ✗ (No)

So 3 is the smallest primitive roots in $\mathbb{Z}^*_{449}$

$3^{42} \bmod 449 \equiv 350 \bmod 449 = 2\cdot 5^2\cdot 7 \bmod 449$

$3^{60} \equiv 36 \bmod 449 = 2^2\cdot 3^2 \bmod 449$

$3^{70} \equiv 22 \bmod 449 = 2\cdot 11 \bmod 449$

$3^{72} \equiv 198 \bmod 449 = 2\cdot 3^2\cdot 11 \bmod 449$

$3^{212} \equiv 195 \bmod 449 = 3\cdot 5\cdot 13 \bmod 449$

let $X(2)$, $X(3)$, $X(5)$, $X(7)$, $X(11)$ and $X(13)$

The distrète logarithm of classes 2, 3, 5, 7, 11 and 13 respectively to base 3 Then $X(3)=1$

$$X(2)+2X(5)+X(7)\equiv 42 \pmod{448}$$

$$2X(2)+2X(3)\equiv 62 \bmod 448$$

$$X(2)+X(11)\equiv 70 \bmod 448$$

$$X(2)+2X(3)+X(11)\equiv 72 \bmod 448$$

$$X(3)+X(5)+X(13)\equiv 212 \bmod 449$$

$X(2)=x$

$X(3)=y$

$X(5)=z$

$X(7)=w$

$X(11)=k$

$X(13)=l$

So solving the above system of modulos we take:

$$\begin{cases} X(2)=30 \\ X(3)=1 \\ X(5)=0 \\ X(7)=12 \\ X(11)=40 \\ X(13)=211 \end{cases}$$

7) Έστω $n = \lceil \log p \rceil$ το μήκος του $p$ σε δυαδική αναπαράσταση. Τότε το $a^x \bmod p$ είναι υπολογίσιμο σε πολυωνυμικό χρόνο $n$. Ωστόσο, δεν υπάρχει γνωστός αλγόριθμος (ντετερμινιστικός) που να μπορεί να υπολογίσει το διακριτό λογάριθμο σε πολυωνυμικό αριθμό βημάτων. Ο καλύτερος αλγόριθμος για τον υπολογισμό του διακριτού λογαρίθμου σε ένα τυχαιοποιημένο σύμπαν τάξης $p$ είναι η μέθοδος του λογισμού δεικτών.

Για εμάς στο δικό μας πρόβλημα ~~θέλω~~ υποθέτουμε ότι $msb_{p,a}(x) = \begin{cases} 0, & x < \frac{p-1}{2} \\ 1, & \text{διαφορετικά} \end{cases}$ ~~διαφορετικά~~

Υποθέτουμε ότι $PRED(p, a, y) \equiv msb_{p,a}(x) \ \forall y$

$LSB(p, a, y) = 1$ εάν $x$ odd αν $0$ $x$ even

Discrete Logarithm $(p, a, y)$:

Αρχικοποιώ $z := y \bmod p \ (= a^x \bmod p)$, $n = |p|$, $i = 1$

Υπολογίζω $b_i := LSB(p, a, z)$

if $b_i = 0 \Rightarrow z = sqrt_p(z)$ ή $z = sqrt(z a^{-1})$

if $PRED(p, a, z) = 1 \rightarrow z = p - z$

if $i < n \rightarrow i = i + 1$ έως 1

αλλιώς έξοδος $b_n, \ldots, b_1$

Άρα εξάγουμε το συμπέρασμα ότι σε πολυωνυμικό χρόνο εάν ο $x$ είναι άρτιος ή περιττός

8)

Λύση

(α) Για να δείξουμε ότι ο 2 είναι πρωτογενής είδη κατά τέτρο $3^n$, θα λύσουμε την ισότητα $2^x \equiv n \bmod 3^n \Rightarrow 2^x n \equiv 1 \bmod 3^n$, $x < 4(3^n)$

Άρα $4(3^n) - x$ είναι η λύση της ισοτήτας.

- Αν $n \equiv 2 \bmod 3$ τότε έχουμε $2^x(2n) \equiv 1 \bmod 3^n$

  $2n \equiv 1 \bmod 3 \Rightarrow x+1$ η λύση

- Αν $n \equiv 1 \bmod 3$ τότε η λύση πρέπει να είναι άρτιος

  $2^{odd} \equiv 2 \bmod 3$

(β) Έχουμε $x = x_0 + 3x_1 + \dots + 3^{n-2} x_{n-2}$

Οπότε $4^{x_0 + 3x_1 + \dots 3} n \equiv 1 \bmod 3^j$ για $j = 1$ ⊛

Έστω $g_1 = 4$ οπότε έχουμε $g_n = 4^{3^{j-1}} \bmod 3^n$

Έχουμε $n_{j-1} g_{j-1}^{x_{j-2}} \equiv (1 - 3^{j-1} x_{j-2}) \cancel{\bmod 3^j}\ g_{j-1}^{x_{j-2}}$

Οπότε $(1+3)^{3^{j-1} x_{j-2}} \equiv 1 + 3^{j-1} x_{j-2} \bmod 3^j$

Άρα το αριστερό μέλος της ⊛ είναι $\equiv (1 - x_j^2 \cdot 3^{2(j-1)}) \equiv 1 \bmod 3^j$

Επομένως αποδείχθη το ζητούμενο.

(γ) Ο αλγόριθμος για την επίλυση της ισοτήτας, θα είναι ως εξής:

Έστω ότι για $j > 1$ έχουμε βρει $x_0 \dots x_{j-3}$ για την ⊛ ώστε να αληθεύει. Υποθέτουμε ότι έχουμε υπολογίσει το $g_{j-1} = 4^{3^{j-2}} \bmod 3^n$ και το $n_{j-2}$. Θέτουμε $x_{j-2} = (1 - n_{j-1}) / 3^{j-1} \bmod 3$.

Παρατηρούμε ότι $n_{j-1} \equiv 1 \bmod 3^{j-1}$ λόγω της ⊛ για $j = j-1$

Έπειτα, υπολογίζουμε $n_j = g_{j-1}^{x_{j-2}} \bmod 3^n$. Τελικά αν $j < n$, υπολογίζουμε το $g_j$ υψώνοντας το στη $3^n$ δύναμη $\bmod 3^n$. Μόλις $j = n$, ο αλγόριθμος σταματάει. Για να υπολογίσουμε τον αριθμό των πράξεων, παρατηρούμε ότι σε κάθε βήμα εκτελείται κάποιος αριθμός πολλαπλασιασμών και διαιρέσεων πολυπλοκότητας $O(n)$ για κάθε bit και $O(n^2)$ για τα bit των πράξεων. Τελικά, έχουμε για τελική πολυπλοκότητα $O(n^3)$.

8) Part 1

a) We have $m \mid b^a - 1$ and $m \mid b^c - 1 \Rightarrow d = (a,c) \Rightarrow \exists\ k, l \in \mathbb{Z}$ (Bezout)

such that $ak + cl = d$. ~~Stra~~ So, $b^d = b^{ak+cl} = (b^a)^k \cdot (b^c)^l \equiv 1 \bmod m$

Hence, $b^a \equiv 1 \bmod m$ and $b^c \equiv 1 \bmod m \Rightarrow m \mid b^d - 1$

b) $\left.\begin{array}{l} p \mid b^a - 1 \\ p \mid b^{p-1} - 1 \end{array}\right\} \Rightarrow p \mid b^\delta - 1 \Rightarrow \delta = (n, p-1)$

if $n \mid p-1 \Leftrightarrow p-1 \bmod n$ So, $p \equiv 1 \bmod n$ and $\delta = n$

if $n \nmid p-1$ zöle $\delta \neq n$ afoi zo $\delta$ ~~Stria~~ is not a divisor of $n, p-1$

and $\delta / n \Rightarrow \delta < n$.