2/12/15

Θεώρημα Wilson
Ο φυσικός $p>1$ είναι πρώτος αν $(p-1)! \equiv -1 \bmod p \equiv p-1 \bmod p$
Αν $m \neq 4$ και σύνθετος, τότε $(m-1)! \equiv 0 \bmod m$
Απόδειξη $\Leftarrow$ $(p-1)! = 1 \cdot 2 \cdots (p-1)$
Έστω $(p-1)! \equiv -1 \bmod p$ (*) και υποθέτουμε ότι ο p δεν είναι πρώτος $\Rightarrow p$ σύνθετος. Άρα υπάρχει $q<p$ πρώτος ώστε $q \mid p \Rightarrow$
Ο q θα βρίσκεται μέσα στο $(p-1)! \Rightarrow q \mid (p-1)!$ $\not\Rightarrow$
και από (*) $\Rightarrow (p-1)! + 1 = kp \Rightarrow q \mid (p-1)! + 1$

$q \mid 1$ Άτοπο!
Ο p είναι πρώτος

$\Rightarrow$ Γνωρίζουμε ότι ο p είναι πρώτος, δείχνουμε $(p-1)! \equiv -1 \bmod p$.
Γνωρίζουμε ότι κάθε κλάση μη-μηδενική στο $\bmod p$ είναι αντιστρέψιμη $\Leftrightarrow \forall\ 1 \le a \le p-1$ & $1 \le b \le p-1$ ώστε $ab \equiv 1 \bmod p$.
Έστω $A = 1 \cdot 2 \cdots (p-1) = (p-1)! \Rightarrow A^2 \equiv 1 \bmod p$
$A^2 \equiv 1 \bmod p$ $A = 1, 2 \ldots (p-1)$
$\Downarrow$
$(A-1)(A+1) \equiv 0 \bmod p \Rightarrow A-1 \equiv 0 \bmod p$
$A+1 \equiv 0 \bmod p$
Αρκεί να δείξουμε ότι $A \neq 1 \bmod p$
Το $A = 1 \cdot 2 \cdots (p-1) \bmod p > 1 \bmod p$
Άρα $A \neq 1 \bmod p$. Θα έχουμε $A \equiv -1 \bmod p$

π.χ. Να δείξετε ότι $\frac{21!}{11!} \equiv -1 \bmod 11$

$\frac{1\cdot 2\cdot \ldots 11\cdot 12\ldots 21}{1\cdot 2\ldots 11} \equiv 12\cdot 13\cdot 21 \bmod 11$

$\equiv (12) \bmod 11 \cdot 13 \bmod 11 \ldots (21) \bmod 11$

$\equiv 1\cdot 2\cdot \ldots 10 \bmod 11 \equiv (11-1)! \bmod 11$

$\equiv -1 \bmod 11$ από Wilson

$(\alpha+\beta)^n = \alpha^n + \sum_{i=1}^{n-1} \binom{n}{i} \alpha^i b^{n-i} + b^n$

$n=p$ πρώτο

$(\alpha+b)^p \bmod p = \left(\alpha^p + \sum_{i=1}^{n-1} \binom{p}{i} \alpha^i b^{p-i} + b^p\right) \bmod p$

$\left.\begin{array}{l} \binom{p}{i} = p \text{ κ για κάθε } p \text{ είναι πρώτος} = 1 \binom{p}{i} \equiv 0 \bmod p \end{array}\right\} \Rightarrow$

$(\alpha+b)^p = (\alpha^p + b^p) \bmod p$

Θεώρημα: Έστω p πρώτος

Τότε $\alpha^p \equiv \alpha \bmod p$. Αν $(\alpha, p)=1$, τότε $\alpha^{p-1} \equiv 1 \bmod p$

Απόδειξη: (Με ισχυρή επαγωγή στο α)

Για $\alpha=1$ και 2 έχουμε $1^p \equiv 1 \bmod p$

$2^p = (1+1)^p \underset{\text{προηγ.}}{=\!=} 1^p + 1^p \bmod p \equiv 2 \bmod p$

Υποθέτουμε ότι ισχύει μέχρι και το α

θα το αποδείξουμε για το $\alpha+1$.

$(\alpha+1)^p \equiv \alpha+1 \bmod p$

$(\alpha+1)^p = (\alpha^p + 1^p) \bmod p \underset{\text{επαγ.}}{\overset{\text{από}}{=\!=}} (\alpha+1) \bmod p$

ισχύει

Αν $(\alpha,p)=1 \Leftrightarrow 0$ α δεν διαιρείται από τον p
$\Rightarrow$ έχει αντίστροφο.
$\exists\, \beta:\ \alpha\beta \equiv 1 \bmod p$
Από το προηγούμενο $\alpha^p \equiv \alpha \bmod p \Rightarrow$
$\beta\alpha^p = \beta\alpha \bmod p \Rightarrow \beta\alpha\cdot\alpha^{p-1} \equiv 1 \bmod p \Rightarrow \alpha^{p-1} \equiv 1 \bmod p$
Τώρα γράψε από εδώ!

ΕΡΩΤΗΜΑ: Αν ο p δεν είναι πρώτος;

Θεώρημα: Έστω α και m φυσικοί θετικοί με
$(\alpha,m)=1$. Τότε $\alpha^{\varphi(m)} \equiv 1 \bmod m$

π.χ. 1) $2^{50}+3^{50} \equiv 0 \bmod 13$
Ο 13 = πρώτος $1<2,3<13$

$2^{\varphi(13)} = 1 \bmod 13 \Leftrightarrow 2^{12} \equiv 1 \bmod 13$
$50 = 12\cdot 4+2 \Rightarrow 2^{50} = 2^{12\cdot 4+2} = (2^{12})^4 \cdot 2^2 = 1^4 \cdot 4 \bmod 13$

$3^{50} = (3^{12})^4 \cdot 3^2 = 1^4 \cdot 9 \bmod 13 \equiv$
άρα $4+9 = 13 = 0 \bmod 13$

2) Να βρεθεί το $3^{372} \bmod 37 = 10 \bmod 37$
37 πρώτος $\varphi^{(37)} = 36$
$372 = 10\cdot 36+12$
$3^{372} \equiv (3^{36})^{10} + 3^{12} \equiv 1\cdot 3^{12} \bmod 37$
$3^2 = 9 \Rightarrow 3^4 = 81 \bmod 37 \equiv 7 \bmod 37$
$3^{12} = (3^4)^3 = 7^3 \bmod 37 = 7\cdot 49 \bmod 37 = 7\cdot 12 \bmod 37 = 84 \bmod 37 =$
$10 \bmod 37$

3) Να δείξετε ότι $7 \nmid n^2+1$

n^2+1 διαιρείται από το 7 $\Leftrightarrow$

$n^2+1 \equiv 0 \bmod 7 \Leftrightarrow n^2 \equiv -1 \bmod 7$

$n^4 \equiv 1 \bmod 7 \Rightarrow n^6 \equiv n^4 \cdot n^2 \equiv 1(-1) \bmod 7$

$n^6 \equiv -1 \bmod 7 \Rightarrow n^{\varphi(7)} \equiv -1 \bmod 7$ ΑΔΥΝΑΤΟ!

$(\alpha, m)=1 \Rightarrow \alpha^{\varphi(m)} \equiv 1 \bmod m \Rightarrow \alpha \cdot \alpha^{\varphi(m)-1} \equiv 1 \bmod m$

Θέλουμε να λύσουμε την $\alpha x \equiv b \bmod m$

$\cdot \alpha^{-1}$ jjjj

Αν $(\alpha, m)=1 \Rightarrow \alpha^{\varphi(m)-1} \cdot \alpha x \equiv \alpha^{\varphi(m)-1} b \bmod m$

$x \equiv \alpha^{\varphi(m)-1} b \bmod m$

Είναι μοναδική;

Θεώρημα. Η ελάχιση $\alpha x \equiv b \bmod m$ έχει λύση στους ακεραίους αν $(\alpha, m) \mid b$

Αν το είναι μια λύση, τότε και οι αριθμοί

$x_0, x_0 + \frac{m}{\delta}, x_0 + \frac{2m}{\delta}, \ldots, x_0 + \frac{(\delta-1)m}{\delta}$ είναι επίσης λύσεις για $\delta = (\alpha, m)$

Αν $(\alpha, m)=1$, τότε η λύση είναι μοναδική: $x \equiv \alpha^{\varphi(m)-1} b \bmod m$

Απόδειξη $\Leftarrow$ $(\alpha, m)=1 \Rightarrow$ έχουμε λύση

$(\alpha, m)=1 \Rightarrow \alpha \alpha^{\varphi(m)-1} = 1 \bmod m \Rightarrow$

$\alpha^{\varphi(m)-1} \alpha x \equiv \alpha^{\varphi(m)-1} b \bmod m \Rightarrow$

$x \equiv \alpha^{\varphi(m)-1} \cdot b \bmod m$

Και είναι μοναδική.

Έστω ότι $(\alpha, m) \mid b \Rightarrow$

Θέλουμε να λύσουμε την $\alpha x \equiv b \bmod m \Leftrightarrow \alpha x - b = km \Leftrightarrow \alpha x - km = b$

Π.χ. Να εξετάσετε αν έχει ακέραιες λύσεις η
$540x \equiv 18 \bmod 462$
$78x \equiv 18 \bmod 462$
Για να έχει λύση πρέπει $(78, 462) \mid 18$

462	78
72	6

$78 = 1 \cdot 72 + 6$
$72 = 12 \cdot 6$
$(462, 78) = 6 \mid 18$ έχουμε λύση

$78x \equiv 18 \bmod 462 \Rightarrow$
$13x \equiv 3 \bmod 77$
$13^{\varphi(77)} = 1 \bmod 77 \Rightarrow 13^{60} \equiv 1 \bmod 77$
$\Rightarrow 13^{-1} \equiv 13^{59} \bmod 77$

$\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11)$
$= 6 \cdot 10 = 60$

Η λύση του Θ είναι $x_0 = 13^{59} \cdot 3 \bmod 77$
Όλες οι λύσεις της αρχικής είναι
$x_0 + \lambda \cdot \frac{462}{6} = x_0 + \lambda \cdot 77$ με $0 \le \lambda \le 5$

$13 \cdot 6 \equiv 78 \bmod 77 \equiv 1 \bmod 77$
Άρα $6 \cdot 13x \equiv 63 \bmod 77 \Rightarrow x_0 \equiv 18 \bmod 77$

$[13]^{-1}_{77} = [y]_{77}$ όπου $y \cdot 13 \equiv 1 \bmod 77$

Π.χ. Να εξετάσετε αν έχει λύση
η $5x \equiv 3 \bmod 24$
$(a, m) = (5, 24) = 1 \mid 3$ έχει λύση
Η λύση μοναδική είναι στις τάξεις
$x_0 = a^{\varphi(m)-1} b \bmod m = 5^{12-1} \cdot 3 \bmod 24 = 5^{7} \cdot 3 \bmod 24$
$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = 2^3 \cdot \varphi(2) \cdot 2 = 8$

$= 5^7 \cdot 3 \bmod 24$

$5^2 = 25 = 1 \bmod 24 \Rightarrow 5^{-1} = 5 \bmod 24$

$5x \equiv 3 \bmod 24 \Rightarrow 5 \cdot 5x = 5 \cdot 3 \bmod 24 \Rightarrow x \equiv 15 \bmod 24$