דינב

בס"ד 12/6/02

תרגילים ~ תורת המספרים האלמנטרית I

$\boxed{1}$ חשב: (i) $5^{10^6} \pmod{144}$ (ii) $(21432, 6666)$

(iii) $(6188, 4709)$ (iv) $2^{90} \pmod{91}$

$\boxed{2}$ פתור את המשוואות:
(i) $7x \equiv 23 \pmod{101}$
(ii) $12x + 21y = 27$
(iii) $22x \equiv 11 \pmod{121}$

$\boxed{3}$ הוכח שלכל n, $30 | n^5 - n$, ולכל n כך ש: $3 \nmid n$ מתקיים $6 | n^2 - 1$.

$\boxed{4}$ הוכח שאם $p = a^n - 1$ ראשוני, אז $a = 2$ ו-n ראשוני (כלומר: p ראשוני של Mersenne). רמז: $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})$

$\boxed{5}$ הוכח שאם $p = a^n + 1$ ראשוני אז a זוגי ו-n חזקה של 2. (ראשוניים מהצורה $2^{2^t}+1$ נקראים ראשוני פרמה – לא ידוע אם יש ∞ כאלו).
רמז: ל-n אי-זוגי, $x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1})$

$\boxed{6}$ סימון: $\nu(n)$ = מס' המחלקים החיוביים של n.
הוכח) שאם: $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ ו-p_i ראשוניים שונים, אזי: $\nu(n) = \prod_{i=1}^{l} (\alpha_i + 1)$
ב) ν פונק' של תורת המספרים

$\boxed{7}$ מצא את כל הפתרונות השלמים חיוביים למשוואה $19x + 20y = 1909$.

$\boxed{8}$ יהי $f(x) = \sum_{i=0}^{n} a_i x^i$ פולינום ב-$\mathbb{Z}[x]$. הוכח שאם קיים $k \in \mathbb{Z}$, d כך ש: $d | f(k+j)$ לכל $j = 0, \dots, d-1$ אזי $d | f(n)$ לכל $n \in \mathbb{Z}$. הראה דוגמא ל-$f(x)$ כזה גם עם: $(a_0, \dots, a_n) = 1$ (כלומר שמקדמי $f(x)$ זרים).

9. הוכח שאם $(a,b)=d$ אז: $\frac{\varphi(ab)}{d} = \frac{\varphi(a)\varphi(b)}{\varphi(d)}$
φ = פונ' אוילר.

10. הוכח עבור $n>1$, סכום השלמים החיוביים הקטנים מ-n וזרים ל-n שווה ל: $\frac{n\varphi(n)}{2}$.

11. הוכח שאם $d|n$ אז $\varphi(d)|\varphi(n)$.

12. פתור את המערכת

$$\begin{cases} x \equiv 1 \ (2) \\ x \equiv 1 \ (3) \\ x \equiv 3 \ (4) \\ x \equiv 4 \ (5) \end{cases}$$

13. הוכח שמספר שלם חיובי מתחלק ב-3 אמ"מ סכום ספרותיו מתחלק ב-3 ומתחלק ב-9 אמ"מ סכום הספרות מתחלק ב-9.

14. הוכח שאם $m=p^\alpha$ לא זוגי $2<p$ ראשוני או: $m=2p^\alpha$ ($2<p$ ראשוני) אז ~~לא~~ הפתרונות היחידים לקונגרואנציה $x^2\equiv 1(m)$ הן ± 1 (מודולו m)
הוכח גם שאם m לא מהצורה הנ"ל אז יש יותר מ-2 פתרונות.

15. (i) הוכח שלכל $k\in\mathbb{Z}$ יש רק מספר סופי של $n\in\mathbb{N}$ כך ש: $\varphi(n)\le k$. (ii) מצא סדרה של $n_i\in\mathbb{N}$ עם $\lim \frac{\varphi(n_i)}{n_i}=1$
וסדרה עם $\lim \frac{\varphi(n_i)}{n_i}=0$

16. יהי F שדה סופי. הוכח שיש ב-$F[x]$ אינסוף פולינומים אי-פריקים (ראשוניים). מצא גם גרסה נוספת להוכחה
ככל האפשר

תורת המספרים - תרגיל 1

(1) חשבו:

(i) $5^{10^6} \pmod{144} = ?$

ידוע שלכל $a \in \mathbb{Z}_n^*$ מתקיים $a^{\varphi(n)} \equiv 1 \pmod{n}$

במקרה שלנו (נתון כ. $n=144$, $a=5$ (וכן $5 \in \mathbb{Z}_{144}^*$

כי 5 ראשוני ! - $5 \nmid 144$ אזי $(5,144)=1$)

$$144 = 2\cdot 72 = 2\cdot 2\cdot 36 = 2\cdot 2\cdot 6\cdot 6 = 2^4\cdot 3^2$$

$$\varphi(144) = 144\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right) = \frac{144}{2}\cdot\frac{2}{3} = 48 \quad \Leftarrow$$

כמו כן, ידוע לנו שאם $m = q\varphi(n)+r$ אז

$$a^{m} = (a^{q})^{\varphi(n)}\cdot a^{r} \equiv a^{r} \pmod{n}$$

נחפש את השארית של החלוקה של 10^6 ב-48:

$$\begin{array}{r} 20833 \\ 1000000 \,|\, 48 \\ \underline{96} \\ 400 \\ \underline{384} \\ 160 \\ \underline{144} \\ 160 \\ \underline{144} \\ 16 \end{array} \quad \Rightarrow \quad 1000000 = 20833\cdot 48 + 16$$

$$\Rightarrow 5^{10^6} \pmod{144} \equiv 5^{16} \pmod{144}$$

$$\equiv (5^4 \pmod{144})^4 \equiv (625 \pmod{144})^4$$

$$\equiv (49^2 \pmod{144})^2 \equiv (2401 \pmod{144})^2$$

$$\equiv 97^2 \pmod{144} \equiv 9409 \pmod{144}$$

$$\equiv 49 \pmod{144}$$

$625 = 4\cdot 144 + 49$

$2401 = 16\cdot 144 + 97$

$9409 = 65\cdot 144 + 49$

(ii) $(21432, 6666) = ?$

נשתמש באלגוריתם אוקלידס:

$$21432 = 3\cdot 6666 + 1434$$

$$6666 = 4\cdot 1434 + 930$$

$$1434 = 1\cdot 930 + 504$$
$$930 = 1\cdot 504 + 426$$
$$504 = 1\cdot 426 + 78$$
$$426 = 5\cdot 78 + 36$$
$$78 = 2\cdot 36 + 6$$
$$36 = 6\cdot 6 \quad \Rightarrow \quad (21432, 6666) = 6$$

(iii) $(6188, 4709) = ?$

$$6188 = 1\cdot 4709 + 1479$$
$$4709 = 3\cdot 1479 + 272$$
$$1479 = 5\cdot 272 + 119$$
$$272 = 2\cdot 119 + 34$$
$$119 = 3\cdot 34 + 17$$
$$34 = 2\cdot 17 \quad \Rightarrow \quad (6188, 4709) = 17$$

(iv) $2^{90} \pmod{91} = ?$

$$\varphi(91) = 6\cdot 12 = 72 \quad \Leftarrow \quad 91 = 7\cdot 13$$

pd $\quad 90 = 1\cdot 72 + 18$

$$2^{90} \pmod{91} \equiv 2^{72+18} \pmod{91} \equiv 2^{18} \pmod{91}$$
$$\equiv (1024 \bmod 91)(256 \bmod 91)$$
$$\equiv (23 \bmod 91)(74 \bmod 91)$$
$$\equiv 1702 \pmod{91} \equiv 64 \pmod{91}$$

$1024 = 11\cdot 91 + 23$
$256 = 2\cdot 91 + 74$

$1702 = 18\cdot 91 + 64$

② נפתור את המשוואות

(i) $7x \equiv 23 \pmod{101}$

נשתמש במשפט: אם $a,n,b \in \mathbb{Z}$ ולמשוואה $ax \equiv b \pmod n$

יש פתרון אמ"מ $b \mid (a,n)$ ובמקרה זה d הפתרונות (מודולו n) הם

$x_0,\ x_0+\frac{n}{d},\ \dots,\ x_0+(d-1)\frac{n}{d}$

כאשר x_0 פתרון פרטי ו- $d=(a,n)$.

במקרה שלנו $a=7$, $b=23$, $n=101$. אז $d=(a,n)=1$

וכמובן $1 \mid 23$. לכן יש פתרון. כדי למצוא את הפתרונות,

נותר למצוא פתרון פרטי: אנחנו רוצים למצוא x רק ש-

$7x \equiv 23 \pmod{101}$ כלומר יש m

$7x+101m=23$

מספיק למצוא x_0,m_0 רק ש- $7x_0+101m_0=1$ כי אז נכפול

הכפלה פי 23 (קבל) את הדרוש. ואכן, מאחר ש- $(7,101)=1$

זה אפשרי. נשתמש באלגוריתם אוקלידס:

$101 = 14\cdot 7+3$

$7 = 2\cdot 3+1$

$3 = 3\cdot 1$

$1 = 7-2\cdot 3 = 7-2(101-14\cdot 7)$

$= 7+2(14\cdot 7-101) = 29\cdot 7-2\cdot 101$

לכן $x=23\cdot 29=667 \Leftarrow x_0=29 \Leftarrow$

הפתרונות הם $667+101k$

(ii) $12x+21y=24$

מספיק לפתור את המשוואה $4x+7y=9$

ממשיים הישר $y=\frac{9-4x}{7}$ מהווה את כל הפתרונות של

המשוואה. אבל אנחנו רוצים פתרונות בשלמים. כלומר

$x,y\in\mathbb{Z} \Rightarrow 9-4x \equiv 0 \pmod 7$

$\Rightarrow -4x \equiv -9 \pmod 7 \Rightarrow 3x \equiv 5 \pmod 7$

7 ראשוני לכן יש פתרון יחיד (מודולו 7) והוא $x=4$

לכן x מהצורה $x = 4+7k$ ומכאן ש-

$$y = \frac{9-4x}{7} = \frac{9-16-28k}{7} = -1-4k$$

$\Leftarrow$ פתרונות המשוואה הם מהצורה $(4+7k, -1-4k)$

(iii) $22x \equiv 11 \pmod{121}$

נשתמש במשפט מהסעיף הראשון. הפעם $a=22$

$b=11$; $n=121$. אז $d=(a,n)=11$ וכמובן

$11|11$. שנותר למצוא פתרון פרטי. נרצה למצוא

x ו- n רק ש- $22x + 121n = 11$

מספיק למצוא $2x + 11n = 1$ זה אפשרי

כי $(2,11)=1$. ברור שאפשר $2\cdot 6 - 11 = 1$

$\Leftarrow$ $x=6$ הוא פתרון פרטי של המשוואה ולכן

הפתרונות הם אז $\{6 + n\cdot 11 + 121k : 0 \le n \le 10, k \in \mathbb{Z}\}$

③ • נוכיח שלכל n, $30 | n^5 - n$

מספיק להוכיח ש- $2|n^5-n$, $3|n^5-n$, $5|n^5-n$

שהרי אז בוודאי $30 = 2\cdot 3\cdot 5 \,|\, n^5-n$.

ברור ש- $2|n^5-n$ משום ש- n, n^5 בעלי אותה זוגיות ולכן הפרשם תמיד זוגי.

כדי להראות ש- $3|n^5-n$ נבחן 3 מקרים:

- $n^5 \equiv 0 \pmod 3 \Leftarrow n \equiv 0 \pmod 3$

  $n^5 - n \equiv 0 \pmod 3 \Leftarrow$

- $n^5 \equiv 1 \pmod 3 \Leftarrow n \equiv 1 \pmod 3$

  $n^5 - n \equiv 0 \pmod 3 \Leftarrow$

- $n^5 \equiv 32 \pmod 3 \equiv 2 \pmod 3 \Leftarrow n \equiv 2 \pmod 3$

  $n^5 - n \equiv 0 \pmod 3 \Leftarrow$

בכל מקרה $3|n^5-n$

באופן דומה, כדי להראות ש- $5|n^5-n$ נבחן 5 מקרים:

- $n^5 \equiv 0 \pmod 5 \Leftarrow n \equiv 0 \pmod 5$

  $n^5 - n \equiv 0 \pmod 5 \Leftarrow$

- $n^5 \equiv 1 \pmod 5 \Leftarrow n \equiv 1 \pmod 5$

  $n^5 - n \equiv 0 \pmod 5 \Leftarrow$

- $n^5 \equiv 32 \pmod 5 \equiv 2 \pmod 5 \Leftarrow n \equiv 2 \pmod 5$

  $n^5 - n \equiv 0 \pmod 5 \Leftarrow$

- $n^5 \equiv 243 \pmod 5 \equiv 3 \pmod 5 \Leftarrow n \equiv 3 \pmod 5$

  $n^5 - n \equiv 0 \pmod 5 \Leftarrow$

- $n^5 \equiv 1024 \pmod 5 \equiv 4 \pmod 5 \Leftarrow n \equiv 4 \pmod 5$

  $n^5 - n \equiv 0 \pmod 5 \Leftarrow$

בכל מקרה $5|n^5-n$ וסיימנו.

• נראה שלכל n אי-זוגי כך ש- $3 \nmid n$ מתקיים $6 | n^2-1$

שוב, מספיק להראות ש- $2|n^2-1$ ו- $3|n^2-1$ גם.

ברור ש- $2|n^2-1$ שהרי n אי-זוגי ולכן n^2 אי-זוגי.

כעת, נניח בשלילה ש- $3 \nmid n^2-1$ אז יש שתי אפשרויות

- $n^2-1 \equiv 1 \pmod 3$ $\Leftarrow$ $n^2 \equiv 2 \pmod 3$. אבל זה

פשוט לא יכול להיות כי אם $n \equiv 1 \pmod 3$ אז

$n^2 \equiv 1 \pmod 3$ ואם $n \equiv 2 \pmod 3$ אז

$n^2 \equiv 1 \pmod 3$ ונתון ש- $n \not\equiv 0 \pmod 3$.

- $n^2-1 \equiv 2 \pmod 3$ $\Leftarrow$ $n^2 \equiv 0 \pmod 3$ וגם זה לא

יכול להיות (מאותו אופן)

לכן בהכרח $6 \mid n^2-1$.

④ נוכיח שאם $p=a^n-1$ ראשוני אז $a=2$ ו-n ראשוני.
[פרט למקרה ש-$n=1$ ואז יש אינסוף אפשרויות ל-a]

אם $n>1$ אז לכל x,y מתקיים

$$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+\dots+xy^{n-2}+y^{n-1})$$

לכן במקרה שלנו,

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

אם p ראשוני אזי $a-1=1$ או $a^{n-1}+a^{n-2}+\dots+a+1=1$

אבל $n>1$ ו-$a\neq 0$ $\Leftarrow$ $a^{n-1}+\dots+a+1>1$

$\Leftarrow$ $a-1=1$ $\Leftarrow$ $a=2$

נניח בשלילה ש-n פריק ונרשום $n=kl$, עבור $k,l\geq 2$. אז

$$p=a^{k\cdot l}-1=(a^k)^l-1=$$
$$=(a^k-1)((a^k)^{l-1}+(a^k)^{l-2}+\dots+a^k+1)$$

ושוב מתקיים בהכרח $a^k-1=1$ $\Leftarrow$ $a^k=2$ וזו
סתירה! $\Leftarrow$ n ראשוני

⑤ נוכיח שאם $p=a^n+1$ ראשוני אז a זוגי ו-n חזקה של 2.
[פרט למקרה ש-$n=1$ ואז יש אינסוף אפשרויות ל-a].

אם $n>1$ אי-זוגי אז לכל x,y מתקיים

$$x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\dots+y^{n-1})$$

לכן במקרה שלנו,

$$p=a^n+1=a^n+1^n=(a+1)(a^{n-1}-a^{n-2}+a^{n-3}-\dots-a+1)$$

! p ראשוני אזי $a+1=1$ או $a^{n-1}-a^{n-2}+\dots-a+1=1$.

אם $a+1=1$ אז $a=0$ וזה לא יכול להיות. אבל
גם $a^{n-1}-a^{n-2}+\dots-a+1=1$ לא יכול להתקיים שהרי

$$\underbrace{a^{n-1}-a^{n-2}}_{>0}+\underbrace{a^{n-3}-a^{n-4}}_{>0}+\dots+\underbrace{a^2-a}_{>0}+1>1$$

לכן בהכרח n זוגי. נאמר $n=2m$ עבור $m\geq 1$. אם
$m=1$ אז n חזקה של 2. אחרת, נתבונן ב-
$p=b^m+1$ כאשר $b=a^2$. באותו אופן נוכיח ש-m

זוגי ואם נמשיך רק באינדוקציה נקבל ש- n חזקה של 2.
נותר להראות ש- a זוגי. אבל זה ברור (פרט למקרה ש-
$a=1$ ו- $p=2$) שהרי אחרת, a^n אי-זוגי ולכן
$p=a^n+1$ זוגי בסתירה לראשוניות.

6) נסמן $\nu(n)$ = מספר המחלקים החיוביים של n
(1) נוכיח שאם $n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ אז $\nu(n)=\prod_{i=1}^{l}(\alpha_i+1)$
המחלקים של n הם מהצורה $p_1^{e_1}\cdots p_l^{e_l}$ כאשר
$0\le e_i\le\alpha_i$ לכל $1\le i\le l$. כל אחת מהאפשרויות כמובן
נותנת מחלק שונה. לכן מספר המחלקים הכולל הוא

$$\nu(n)=\prod_{i=1}^{l}(\alpha_i+1)$$

(2) נוכיח ש- ν פונקציה של תורת המספרים. כלומר להוכיח
שאם $(m,n)=1$ אז $\nu(mn)=\nu(m)\nu(n)$,
אבל זה נובע ישירות מסעיף הקודם שהרי אם נסמן
$n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ $\quad m=q_1^{\beta_1}\cdots q_k^{\beta_k}$
אז אם $(m,n)=1$ אז כל $p_1,\dots,p_l,q_1,\dots,q_k$ שונים
ולכן $mn=p_1^{\alpha_1}\cdots p_l^{\alpha_l}q_1^{\beta_1}\cdots q_k^{\beta_k}$ ואז

$$\nu(mn)=\prod_{i=1}^{l}(\alpha_i+1)\prod_{i=1}^{k}(\beta_i+1)=\nu(n)\nu(m)$$

(7) נמצא את φ הפתרונות השלמים החיוביים למשוואה $19x+20y=1909$

פל $\mathbb{R}$ הפתרונות נתונים ע״י $y=\frac{1909-19x}{20}$. אבל אנחנו רוצים פתרונות שלמים אז נחפש x-ים כך ש-

$$1909-19x \equiv 0 \pmod{20}$$

$$\Rightarrow 19x \equiv 1909 \pmod{20}$$

$$\Rightarrow 19x + 20n = 1909$$

מאחר ש- $(19,20)=1$ אפשר למצוא x_0, n_0 כך ש- $19x_0+20n_0=1$ וע״י הכפלה ב-1909 נמצא x נחוץ.

כמובן $19\cdot(-1)+20\cdot 1$. לכן $x=-1909$ מקיים את הדרוש. אכן הפתרון הכללי הינו

$$(-1909+20k\ ,\ 1909-19k)$$

אנחנו מעוניינים בפתרונות חיוביים, לכן שני הרכיבים חיוביים.

• $-1909+20k>0 \Leftarrow 20k>1909$

$\Leftarrow k>95.45 \Leftarrow k\geq 96$

• $1909-19k>0 \Leftarrow 1909>19k$

$\Leftarrow k<100.474 \Leftarrow k\leq 100$.

לכן הפתרונות הם

$(11, 85)$ $(71, 28)$

$(31, 66)$ $(91, 9)$

$(51, 47)$

(8) יהי $f(x)=\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[X]$. נניח שקיימים $d,k \in \mathbb{Z}$ כך
ש- $d \mid f(k+j)$ לכל $j=0,\dots,d-1$. נוכיח שאז
$d \mid f(m)$ לכל $m \in \mathbb{Z}$.

אפשר לרשום $m = dq + k + j$ עבור $0 \le j \le d-1$ כלשהו
מאחר ש- $d \mid f(k+j)$ מספיק להראות ש- $d \mid f(m) - f(k+j)$
נסמן $\alpha = k+j$ ואז $f(m)-f(k+j) = f(qd+\alpha) - f(\alpha)$
אז

$$f(m)-f(k+j) = \sum_{i=0}^{n} a_i (qd+\alpha)^i - \sum_{i=0}^{n} a_i \alpha^i =$$

$$= \sum_{i=0}^{n} a_i \left[\sum_{j=0}^{i} \binom{i}{j} (qd)^j \alpha^{i-j} \right] - \sum_{i=0}^{n} a_i \alpha^i$$

$$= \sum_{i=0}^{n} a_i \left[\alpha^i + \text{איברים שמתחלקים ב-}d \right] - \sum_{i=0}^{n} a_i \alpha^i$$

$$= \sum_{i=0}^{n} a_i \alpha^i + \sum_{i=0}^{n} a_i \left(\text{איברים שמתחלקים ב-}d \right) - \sum_{i=0}^{n} a_i \alpha^i$$

$$= \sum_{i=0}^{n} a_i \left(\text{איברים שמתחלקים ב-}d \right)$$

וזה מספר שמתחלק ב-d כפי שטענו.

המסקנה אפשרית גם אם המקדמים של הפולינום זרים. למשל,
נתבונן בפולינום $f(x) = 11x^4 + 3x^3 + 5x^2 + 7x + 1$
אם $d=2$ ו- k כלשהו. קל לראות שלכל $a \in \mathbb{Z}$,
$f(a)$ לא אכן מתחלק ב-2. אבל מקדמי הפולינום
זרים...

9 נוכיח שאם $(a,b)=d$ אז $\frac{\varphi(ab)}{d}=\frac{\varphi(a)\varphi(b)}{\varphi(d)}$

יהיו $\begin{cases} a=p_1^{\alpha_1}\cdots p_l^{\alpha_l}q_1^{\beta_1}\cdots q_k^{\beta_k} \\ b=p_1^{\gamma_1}\cdots p_l^{\gamma_l}r_1^{\delta_1}\cdots r_n^{\delta_n}\end{cases} \Rightarrow d=p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l}$

ולכן:

$$\frac{\varphi(ab)}{d}=\frac{ab\prod(1-\frac{1}{p_i})\prod(1-\frac{1}{q_i})\prod(1-\frac{1}{r_i})}{d}=$$

$$=\frac{a\prod(1-\frac{1}{p_i})\prod(1-\frac{1}{q_i})b\prod(1-\frac{1}{p_i})\prod(1-\frac{1}{r_i})}{d\cdot\prod(1-\frac{1}{p_i})}=$$

$$=\frac{\varphi(a)\varphi(b)}{\varphi(d)}$$

10 נוכיח שעבור $1<n$ סכום השלמים החיוביים הקטנים מ-n וזרים ל-n שווה ל- $\frac{n\cdot\varphi(n)}{2}$.

עבור $n=2$ זה נכון כי 1 הוא המספר היחיד המקיים את הדרוש ומתקיים $\frac{2\cdot\varphi(2)}{2}=\varphi(2)=1$

אם $2<n$ אז $\varphi(n)$ זוגי שהרי אם $n=p_1^{r_1}\cdots p_k^{r_k}$ אז $\varphi(n)=p_1^{r_1-1}(p_1-1)\cdots p_k^{r_k-1}(p_k-1)$

אם n חזקה של 2 אז $\varphi(n)$ חזקה של 2. אחרת, יש ב-n גורם ראשוני אי-זוגי ולכן ב-$\varphi(n)$ מופיע גורם זוגי.

כעת, נשים לב שאם $(a,n)=1$ אז גם $(n-a,a)=1$

שהרי אם $d|a$; $d|n-a$ אז $d|n$ ולכן $d|(a,n)$ ולכן $d=1$.

נסמן: $\Phi(n)$ את קבוצת השלמים החיוביים הקטנים מ-n וזרים לו.

אז אפשר לחלק את איברי $\Phi(n)$ לזוגות - $(a,n-a)$

סכום כל זוג הוא n ויש $\frac{\varphi(n)}{2}$ זוגות. לכן סה״כ הסכום הוא $\frac{n\varphi(n)}{2}$.

(11) נוכיח שאם $d|n$ אז $\varphi(d)|\varphi(n)$

נסמן $n = p_1^{\alpha_1}\cdots p_l^{\alpha_l} q_1^{\beta_1}\cdots q_k^{\beta_k}$; $d = p_1^{\gamma_1}\cdots p_l^{\gamma_l}$. אז

$$\frac{\varphi(n)}{\varphi(d)} = \frac{n\cdot \cancel{\prod_{i=1}^{l}(1-\frac{1}{p_i})}\prod(1-\frac{1}{q_i})}{d\cdot \cancel{\prod(1-\frac{1}{p_i})}} =$$

$$= p_1^{\alpha_1-\gamma_1}\cdots p_l^{\alpha_l-\gamma_l}\cdot q_1^{\beta_1-1}(q_1-1)\cdots q_k^{\beta_k-1}(q_k-1) \in \mathbb{Z}$$

(12) נפתור את המערכת

1) $x \equiv 1 \pmod 2$

2) $x \equiv 1 \pmod 3$

3) $x \equiv 3 \pmod 4$

4) $x \equiv 4 \pmod 5$

מ-(3) נובע ש-x מהצורה $x = 4k+3$ (ולכן זה מקיים את (4).

לפי (2) $k \not\equiv 0 \pmod 3$, $k \not\equiv 2 \pmod 3$ ולכן

בהכרח $k \equiv 1 \pmod 3$ $\Leftarrow$ $k = 3k+1$

$\Leftarrow$ $x = 4(3k+1)+3 = 12k+7$.

לפי (4), $k \not\equiv 0 \pmod 5$, $k \not\equiv 2 \pmod 5$, $k \not\equiv 3 \pmod 5$,

$k \not\equiv 4 \pmod 5$. ולכן בהכרח $k \equiv 1 \pmod 5$

$\Leftarrow$ $k = 5k+1$ $\Leftarrow$ $x = 12(5k+1)+7 = 60k+19$

60 מתחלק ב- 2,3,4,5 ולכן כדי להוכיח ש-x פתרון

צריך לבדוק את השאריות של 19. אכן -

$19 \equiv 1 \pmod 2$ $\quad 19 = 2\cdot 9+1$

$19 \equiv 1 \pmod 3$ $\quad 19 = 3\cdot 6+1$

$19 \equiv 3 \pmod 4$ $\quad 19 = 4\cdot 4+3$

$19 \equiv 4 \pmod 5$ $\quad 19 + 3\cdot 5 + 4$

(B) • נוכיח שמספר שלם חיובי מתחלק ב-3 אמ"מ סכום ספרותיו מתחלק ב-3.
נוכיח טענה חזקה יותר: נראה שהשארית בחלוקת m ב-3 שווה
לשארית בחלוקת סכום הספרות של m ב-3.
נראה באינדוקציה על מספר הספרות ב-m. נסמן $m=a_1a_2\dots a_n$
אם $n=1$ הטענה ברורה. נניח ל-n ונוכיח ל-$n+1$. יש 3 אפשרויות:

- $a_{n+1}\equiv 0 \pmod 3$. אז סכום הספרות נשאר כפי שהיה ואז:
$a_1\dots a_{n+1}=10a_1\dots a_n+a_{n+1}$ אם $a_1\dots a_n\equiv 0 \pmod 3$ אז
$a_1\dots a_{n+1}\equiv 0 \pmod 3$ והטענה נכונה. אם $a_1\dots a_n\equiv 1 \pmod 3$
אז $a_1\dots a_{n+1}\equiv 10 \pmod 3$ וזה שווה ל-1 מודולו 3 ולכן
הטענה נכונה. אם $a_1\dots a_n\equiv 2 \pmod 3$ אז $a_1\dots a_{n+1}\equiv 20 \pmod 3$
וזה שווה ל-2 מודולו 3 והטענה נכונה.
- $a_{n+1}\equiv 1 \pmod 3$ אז סכום הספרות גדל ב-1 שלם.
$a_1\dots a_{n+1}=10a_1\dots a_n+a_{n+1}$. לכן, אם $a_1\dots a_n\equiv 0 \pmod 3$ אז
$a_1\dots a_{n+1}\equiv a_{n+1} \pmod 3$ וזה 1 וגם סכום הספרות הוא 1 מודולו 3.
אם $a_1\dots a_n\equiv 1 \pmod 3$ אז סכום הספרות הוא 2 מודולו 3
וגם $a_1\dots a_{n+1}\equiv 11 \pmod 3 \equiv 2 \pmod 3$. ולבסוף, אם
$a_1\dots a_n\equiv 2 \pmod 3$ אז סכום הספרות הוא 0 מודולו 3 וגם
$a_1\dots a_{n+1}\equiv 21 \pmod 3 \equiv 0 \pmod 3$
- $a_{n+1}\equiv 2 \pmod 3$ אם $a_1\dots a_n\equiv 0 \pmod 3$ אז סכום הספרות הוא
2 מודולו 3 ; $a_1\dots a_{n+1}\equiv a_{n+1} \pmod 3 \equiv 2 \pmod 3$
אם $a_1\dots a_n\equiv 1 \pmod 3$ אז סכום הספרות הוא 0 מודולו 3 ;
$a_1\dots a_{n+1}\equiv 12 \pmod 3 \equiv 0 \pmod 3$ ואם $a_1\dots a_n\equiv 2 \pmod 3$ אז
סכום הספרות הוא 1 מודולו 3 וגם $a_1\dots a_{n+1}\equiv 22 \pmod 3 \equiv 1 \pmod 3$

• מספר שלם חיובי מתחלק ב-9 אמ"מ סכום ספרותיו מתחלק ב-9.
ההוכחה באותו אופן כמו במקרה של 3.

(14) נוכיח שאם $m=p^\alpha$ או $m=2p^\alpha$ עבור $2<p$ ראשוני אז
הפתרונות היחידים למשוואה $x^2\equiv 1 \pmod m$ הם ± 1 (מודולו m).

ראשית נתבונן במקרה $m=p^\alpha$. נניח ש- $x^2\equiv 1 \pmod m$
אז ב- $\mathbb{Z}_m$ מתקיים $0=(x-1)(x+1)=x^2-1$. אז $x-1$
ו- $x+1$ מחלקי אפס ב- $\mathbb{Z}_m$. אבל מחלק אפס ב- $\mathbb{Z}_m$ יכול להיות
רק k כך ש- $(k,m)\neq 1$. אז $x+1$, $x-1$ אינם זרים ל- p^α.
לכן $p\mid x+1$; $p\mid x-1$. כלומר $x+1=pk$;

$$pn+1=x=pk-1 \Leftarrow x-1=pn$$

$\Leftarrow$ $p(k-n)=2$ וזה לא יכול להיות כי מהמשוואה $k\neq n$; ו- $p>2$.
לכן אין מחלקי אפס שאינם אפס $\Leftarrow$ $x=\pm 1$.

באופן דומה, אם $m=2p^\alpha$ אז לכן ש- $x-1$, $x+1$ אינם זרים
ל- $2p^\alpha$. צריך לבחון כמה אפשרויות:
- אם $x-1=pn$; $x+1=pk$ מתקבלת סתירה באותו אופן.
- אחרת, $x-1$; $x+1$ זוגיים. נניח ש- $(x-1)(x+1)=2p^\alpha k$.

כמו קודם לא יכול להיות שגם $p\mid x+1$ וגם $p\mid x-1$ ולכן
מפירוק לגורמים p^α שייך רק ל- $x+1$ או $x-1$ אבל גם מכאן
ששניהם זוגיים בפירוק לגורמים מופיע ה-2 יחד עם ה- p^α.
אז למשל נניח ש- $2p^\alpha$ מופיע ב- $x-1$. אז $x-1=2p^\alpha n$. אבל
$2p^\alpha=m$, אז $x-1=mn$. אבל זה אומר שב- $\mathbb{Z}_m$, $x-1=0$.
$\Leftarrow$ $x=1$. באותו אופן משתמשים במקרה ש- $x+1=2p^\alpha n$.

אם m לא מהצורה הנ"ל אז יש יותר מ-2 פתרונות. מספיק להוכיח למקרה של
$m=p^\alpha q^\beta$ כי אם יש יותר משני גורמים אפשר לצמצם ב- $\mathbb{Z}_m$ את $\mathbb{Z}_{p^\alpha q^\beta}$.
ידוע ש- $\mathbb{Z}_m \cong \mathbb{Z}_{p^\alpha}\times\mathbb{Z}_{q^\beta}$. בכל אחד מ- $\mathbb{Z}_{p^\alpha}$, $\mathbb{Z}_{q^\beta}$ יש שני פתרונות
למשוואה לפי השאלה הקודמת. הדבר שלהם נותן ארבעה פתרונות שונים.

(15) (i) נוכיח שלכל $k\in\mathbb{Z}$ יש רק מספר סופי של $n\in\mathbb{N}$ כך ש-

$$\varphi(n)\le k$$

מספיק להראות שלכל $n>6$, $\varphi(n)\ge\sqrt{n}$. נוכיח זאת בשלבים.

עבור $p\ge3$ ראשוני מתקיים $\varphi(p)=p-1\ge\sqrt{p}$. כעת, אם

$\varphi(p^\alpha)=p^{\alpha-1}(p-1)\ge\sqrt{p^\alpha}$ אז

$$\varphi(p^{\alpha+1})=p^\alpha(p-1)=p^{\alpha-1}p(p-1)\ge p^{\alpha-1}(p-1)\sqrt{p}\ge\sqrt{p^\alpha}\sqrt{p}=\sqrt{p^{\alpha+1}}$$

$\Leftarrow$ באינדוקציה לכל $p\ge3$ ולכל $\alpha\in\mathbb{N}$ $\varphi(p^\alpha)\ge\sqrt{p^\alpha}$. בנוסף

מהכפליות של φ ושל $\sqrt{\cdot}$ נובע שלכל $n\in\mathbb{N}$ שלא מופיעים בפירוק שלו 2 או 3

מתקיים $\varphi(n)\ge\sqrt{n}$. באותו אופן $\varphi(2^\alpha)\ge\sqrt{2^\alpha}$; $\varphi(3^\alpha)\ge\sqrt{3^\alpha}$

ל- $\alpha\ge2$. נותר לטפל במקרה ש-2 או 3 מופיעים בפירוק של n בחזקה 1.

נניח שב-k לא מופיע 2 וגם לא 3 אז $\varphi(3k)=\varphi(3)\varphi(k)=2\varphi(k)\ge2\sqrt{k}\ge\sqrt{3k}$

אם ב-k לא מופיע 2 אז מספיק להוכיח למקרה $k=p^\alpha$ ואז להשתמש

בכפליות. אם $p=3$ אז בהכרח $\alpha\ge2$ ואז $\varphi(2\cdot3^2)=6\ge\sqrt{18}$

וגם אפשר להמשיך מאינדוקציה אם $p>3$ אז בוודאי $\varphi(2p)>\sqrt{2p}$

ובאינדוקציה זה נובע לכל $k=p^\alpha$ סיימנו

(ii) יש סדרה של $n_i\in\mathbb{N}$ כך ש- $\lim_{i\to\infty}\frac{\varphi(n_i)}{n_i}=1$ למשל $n_i=p_i^i$

כאשר p_i הראשוני ה-i אז

$$\frac{\varphi(n_i)}{n_i}=\frac{p_i^{i-1}(p_i-1)}{p_i^i}=\frac{p_i-1}{p_i}=1-\frac{1}{p_i}\longrightarrow1$$

ויש סדרה של $n_i\in\mathbb{N}$ כך ש- $\lim_{i\to\infty}\frac{\varphi(n_i)}{n_i}=0$ למשל $n_i=p_1\cdots p_i$

אז $$\frac{\varphi(n_i)}{n_i}=\frac{n_i\prod(1-\frac{1}{p_i})}{n_i}=\prod\left(1-\frac{1}{p_i}\right)\longrightarrow0$$

והגבול נכון לפי המשפט: $\prod_{i=1}^{\infty}(1-\varepsilon_i)=0$ אמ"מ $\sum_{i=1}^{\infty}\varepsilon_i=\infty$

והרי אנחנו יודעים ש- $\sum_{i=1}^{\infty}\frac{1}{p_i}=\infty$

(16) יהי F שדה סופי. נראה שיש ב- $F[X]$ אינסוף פולינומים אי-פריקים.
הטענה נכונה גם לשדה אינסופי אלא ששם היא טריוויאלית: $x-a$
הוא אי-פריק לכל $a \in F$.
נניח שיש מספר סופי של פולינומים אי-פריקים $f_1,\dots,f_k \in F[X]$
ונתבונן ב- $g = f_1 \cdots f_k + 1$. g מתפרק למכפלת גורמים
אי-פריקים אלא שאף אחד מהגורמים לא יכול להיות $f_1,\dots,f_k$
כי $g \equiv 1 \pmod{f_i}$ לכל $1 \le i \le k$. לכן חייב
להיות פולינום אי-פריק שאינו $f_1,\dots,f_k$.
נמצא הערכות כמותיות למספר הפולינומים

ג3 תרגיל מס' 2 בקורס תורת המספרים וקריפטוגרפיה

1) הוכח שיש אינסוף ראשוניים מהצורה $4k+1$.
רמז: זכור ש: $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$. אם $p_1,\dots,p_l$ ראשוניים עם $p_i\equiv 1(4)$ התבונן ב: $N=(2p_1\cdot\ldots\cdot p_l)^2+1$ ומצא מיהם הראשוניים p המחלקים אותו.

2) הוכח שיש אינסוף ראשוניים מהצורה $8k+7$.
רמז: זכור ש: $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$ והתבונן ב-: $N=(4p_1p_2\cdot\ldots\cdot p_l)^2-2$. נניח p ראשוני אי-זוגי המחלק אותו. הוכח שלא יתכן שכולם מהצורה $p\equiv 1(8)$.

3) יהא $a\in\mathbb{Z}$ שלם שאינו ריבוע של שלם אחר. הוכח שיש אינסוף ראשוניים p כך ש: $\left(\frac{a}{p}\right)=-1$.

4) יהיו $r_1,r_2,\dots,r_{(p-1)/2}$ השאריות הריבועיות מודולו p (ראשוני אי-זוגי). הוכח שמכפלתם שווה ל-1 (מודולו p) אם $p\equiv 3(4)$ וזה $-(-1)$ (מודולו p) אם $p\equiv 1(4)$.

5) תאר את כל הראשוניים p ש-7 הוא שארית ריבועית מודולו p.

6) תאר את כל הראשוניים p ש-15 הוא שארית ריבועית מודולו p:

7) חשב (בעזרת סמל יעקובי) את:

$$\left(\frac{113}{997}\right),\ \left(\frac{215}{761}\right),\ \left(\frac{514}{1093}\right),\ \left(\frac{401}{757}\right)$$

8) נניח p ראשוני ו: $p\equiv 1(4)$. הוכח שיש שלמים s ו-t כך ש: $pt=1+s^2$. הסק מכאן ש-p אינו ראשוני בחוג $\mathbb{Z}[i]$. (זכור ש-$\mathbb{Z}[i]$ חוג אוקלידי עם פריקות יחידה לראשוניים!)

9) בהמשך לתרגיל 8: הסק גם שאם $p\equiv 1(4)$ אז p ניתן להצגה כ: $p=a^2+b^2$ כאשר a ו-b שלמים (רמז: רשום $p=\alpha\cdot\beta$, $\alpha,\beta\in\mathbb{Z}[i]$ והם לא הפיכים שם עפ"י 8).
— הוכח שאם $p\equiv 3(4)$ אז p אינו ניתן להצגה כ: $p=a^2+b^2$.

10) השתמש בתרגיל 4 בקובץ תרגילים מס. I – כדי להוכיח ש-3 אינו שארית ריבועית מודולו p אם p הוא ראשוני של Mersenne.

11) $a\in\mathbb{Z}$ נקרא פרימיטיבי מודולו p, אם (p ראשוני כמובן) $p\nmid a$ ו-a יוצר את החבורה $(\mathbb{Z}/p\mathbb{Z})^*$. הוכח שאיבר פרימיטיבי אינו יכול להיות שארית ריבועית.
— האם כל איבר שאינו שארית ריבועית הוא פרימיטיבי?

12) א) הוכח שאם p הוא ראשוני של פרמה (כלו' ראשוני מהצורה $p=2^{2^t}+1$; ראה תרגיל 5 בקובץ תרגילים מס. I) אז $a\in\mathbb{Z}$ הוא פרימיטיבי מודולו p אם ורק אם a אינו שארית ריבועית.
ב) הוכח שתכונה זו מאפיינת את הראשוניים של פרמה.

13) חזור לתרגיל 3 בקובץ תרגילים I: הוכח בשנית את התרגיל. הראה ש-... איננו. (תוצאה לגבי ההפוך).

דף תרגילים מס' 3

1) א) הוכח שלמשוואה $a_1x_1+\dots+a_nx_n=b$

כאשר $a_1,\dots,a_n,b\in\mathbb{Z}$ יש פתרון מעל השלמים

(כלו' יש $x_1,\dots,x_n\in\mathbb{Z}$ המקיימים אותה) אמ"מ יש

פתרון מודולו m לכל $0<m\in\mathbb{Z}$

ב) הוכח את הבעיה הגלובלית עבור מערכת משוואות לינארית.

2) הסבר מדוע למרות שלמשוואה:

$$(X^2-13)(X^2-17)(X^2-221)\equiv 0 \pmod m$$

יש פתרון מודולו m לכל m שלם, אבל אין לה פתרון מעל השלמים.

3) יהי p ראשוני, $p\neq 2$, ונתבונן בתבנית הריבועית:

$$(*)\quad f(x,y)=ax^2+2bxy+cy^2$$

הדיסקרימיננטה של התבנית: $d=ac-b^2$

טענה: הוכח שלמשוואה $f(x,y)\equiv 0 \pmod p$ יש פתרון שונה מ-0 אמ"מ אז: $-d\equiv 0(p)$ או: $\left(\frac{-d}{p}\right)=1$.

הדרכה: ל-(*) יש פתרון אמ"מ קיים וקטור $0\neq v=\binom{x}{y}$ ב-$\mathbb{F}_p^2$ כך ש: $v^tAv=0$, כאשר: $A=\begin{pmatrix} a & b\\ b & c\end{pmatrix}$

הוכח ש-A שקולה לאלכסונית רגילה: זה קיים מטריצה הפיכה C כך ש: $C^tAC=\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}=A'$ ושקילות משנה הדיסקרימיננטה בהכפלה בריבוע רגיל. לכן תבניות שקולות לתבנית

$f'(x,y)=\alpha x^2+\beta y^2$ לגלות שלו יש פתרון שונה מ-0.

עם $d'=\alpha\beta$ ומסקן להוכיח שלכלה יש פתרון.

אם $\alpha\beta=0$ ~~ברור~~ f_1.

אם $\alpha\beta\neq 0$ ש שקול לפתרון $-d=\left(\frac{\beta y}{x}\right)^2 \pmod p$.

4) הוכח שסדרת המספרים הp-אדיים הסדרה $x_n=1+p+\dots+p^{n-1}$ מתכנסת ל $\frac{1}{1-p}$.

5) הוכח שלמשוואה $f(x)\equiv 0 \pmod{p^n}$ יש פתרון לכל n (פולינום) אזי יש לה פתרון בחוג המספרים הp-אדיים השלמים.

6) רשום את המספר $\frac{2}{3}$ בחוג $\hat{\mathbb{Z}}_5$ של המספרים השלמים ה 5-אדיים (כלומר

בצורה $\sum_{i=0}^{\infty} a_i 5^i$, $0\le a_i<5$

7) הוכח שבחוג $\hat{\mathbb{Z}}_p$ אין איבר $x\neq 1$ המקיים $x^p=1$.

8) הוכח שבמספרים הp-אדיים הטור $\sum_{i=1}^{\infty}\alpha_i$ מתכנס אם"ם $\lim_{i\to\infty}\alpha_i=0$

9) אם $p\neq 2$ אזי: $\alpha\in\hat{\mathbb{Z}}_p$ כך ש: $\alpha\equiv 1 \pmod p$

אזי ל-α יש שורש ב-$\hat{\mathbb{Z}}_p$.

יותר כללי: אם $\alpha=\sum_{n=0}^{\infty} a_n p^n$ אזי ל-α יש שורש ריבועי ב-$\hat{\mathbb{Z}}_p$ אם"ם $\left(\frac{a_0}{p}\right)=1$.