PROBLEMS NUMBER THEORY

1

$a^n + b^n = c^n$

PLAN OF ALGEBRA

- REVISION OF INEQUALITIES
- FUNCTIONAL EQUATIONS
- POLYNOMIALS
- SEQUENCES

Problem 57

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

Proof

$\{1, 2, 3, \dots, p-1\}$ there are exactly $\frac{p-1}{2}$ q. residues and $\frac{p-1}{2}$ q. n. residues.

Quadratic residues are exactly $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ mod $p$

$$= \frac{p-1}{2} \cdot 1 + \frac{p-1}{2} \cdot (-1) = 0$$

Prove that $3^n + 1$ has no prime divisor of the form $12k+11$.

$$\frac{12k+11}{35} \rightsquigarrow \begin{matrix}5\\7\end{matrix}$$

(2)

HINT
- even
- odd

Even $n = 2k$, $p = 12k+11$, $p \mid 3^{2k}+1 \Rightarrow$

$(3^k)^2 \equiv -1 \pmod{p}$

1) • $p \mid (3^k)^2 + 1^2$ and $p = 4\ell+3$ ↯

2) $\left(\frac{-1}{p}\right) = 1$, $(-1)^{\frac{p-1}{2}} = 1 \Rightarrow (-1)^{\frac{12k+11-1}{2}} = 1$ ↯

$(-1)^{6k+5}$

- $n = 2k+1$

$$3^{2k+1} \equiv -1 \pmod{p} \Rightarrow \left(3^{k+1}\right)^2 \equiv -3 \pmod{p}, \text{ so}$$

$\left(\frac{-3}{p}\right) = 1$, by Problem 53 ↯ (3)

$= -1$ if $12k+11$

<u>Problem 59</u> (Polish Final TST) $6a \mid b^2+a+3$, $a \neq 0$. Prove $a<0$

$3^2+3+3 \to 15$

$$\underbrace{b^2+a+3}_{>} = 6\underbrace{a}_{>0}\cdot\underbrace{k}_{>0} \qquad k \geq 1$$

Suppose <u>$a>0$</u>

$$\underbrace{b^2+3}_{>0} = 6a\cdot k - a = \boxed{\underbrace{a}_{>}\underbrace{(6k-1)}_{>}} \quad \text{and ?...}$$

so $p \equiv -1 \pmod{6}$ $p \mid 6k-1$. so $b^2+3 \equiv 0 \pmod{p} \rightsquigarrow$

$\rightsquigarrow \left(\frac{-3}{p}\right) = 1$ when $p \equiv -1 \pmod{6}$ ↯ Problem $\boxed{53}$

key point was $6k-1$, $k=-\ell$, $\ell>0$.

$6k-1 = -6\ell-1 = -(6\ell+1)$

$\ell>0$



$\underline{a>0} \leadsto$ ↯ so $\underline{a<0}$.

<u>Problem 60</u> $\underline{x_1=7}$ and

$x_{n+1} = 2x_n^2-1$. Prove $2003 \nmid x_n$ for any $n$!

2003 is a prime :)

Suppose for some $n$: $2003 \mid x_{n+1}$ then

$$2x_n^2-1 \equiv 0 \pmod{2003}$$

$$2x_n^2 \equiv 1 \pmod{2003} \cdot 2$$

$$(2x_n)^2 \equiv 2 \pmod{2003} \Rightarrow \left(\frac{2}{2003}\right) = 1.$$

<u>But</u> $\left(\frac{2}{2003}\right) = (-1)^{\frac{2003^2-1}{8}} = (-1)^{501501} = -1.$ ↯

$2x_4^2 \equiv 1 \mod 2003 \mid 1002$.

$\underbrace{2004}_{1} \cdot x_4^2 \equiv 1002 \pmod{2003}$

$x_4^2 \equiv 1002 \mod(2003) \Rightarrow \left(\frac{1002}{2003}\right) = 1$.

$\Downarrow$

$-1$

$\lightning$

5

$\left(\frac{2}{2003}\right)$

<u>Thue's lemma</u> $n, a,$ s.t $(n,a) = 1$. Then there exist

$0 < x, y \leq \sqrt{n}$ s.t

$ax \equiv \pm y \pmod{n}$.

$p = x^2 + xy + y^2$

6

1) $x^2 \equiv 0, 1 \mod 3$

Suppose $3 \mid x$, then $p \equiv 0 + 0 + (0 \vee 1) \mod 3$

$\Downarrow$

$p = 3$ or $p \equiv 1 \mod 3$

Assu $3 \nmid x$, $3 \nmid y$ then

$p \equiv 1 + xy + 1 \mod 3 \equiv 0, 1 \mod 3$

$x, y \equiv 1, 2$

2) $p \mid 4x^2 + 4xy + 4y^2 = (2x+y)^2 + 3y^2 \Rightarrow$

$(2x+y)^2 \equiv -3y^2 \mod p \mid : y^2$

$((2x+y) \cdot y^{-1})^2 \equiv -3 \Rightarrow \left(\frac{-3}{p}\right) = 1 \Rightarrow$

$\Rightarrow p = 3k + 1$.

$\cancel{p>3}$ $\quad p = 3k+1 \overset{S3}{\Longrightarrow} \left(\frac{-3}{p}\right) = 1$. so there is $a$ s.t

$p \mid 3+a^2$, $a^2 \equiv -3 \pmod p \Rightarrow (a,p) = 1$.

so by Thue's lemma: $\exists$ $0 < x, y < \sqrt{p}$, $\mathbb{Z}$ s.t $\quad$ (1)

$$ax \equiv \pm y \pmod p$$

$$a^2x^2 \equiv y^2 \pmod p \Rightarrow -3x^2 \equiv y^2 \bmod p \text{ so}$$

$p \mid 3x^2+y^2$. But

$$0 < 3x^2+y^2 < 3(\sqrt{p})^2 + (\sqrt{p})^2 = 4p \text{ so}$$

$3x^2+y^2 = p, 2p, 3p$.

We need $p = a^2+ab+b^2$ for some $a, b$ integers.

1) $p = 3x^2 + y^2 = \underbrace{(y-x)^2}_{a^2} + \underbrace{(y-x)}_{a} \cdot \underbrace{2x}_{b} + \underbrace{(2x)^2}_{b}$ V

$p = b^2$

8

2) $2p = 3x^2 + y^2 \rightsquigarrow x, y$ have the same parity, so

$4 \mid 3x^2 + y^2 = 2p$ ↯ X

3) $3p = 3x^2 + y^2 \Rightarrow 3 \mid y^2 \Rightarrow y = 3y_1$, so V

$3p = 3x^2 + 9y_1^2 \Rightarrow \boxed{p = x^2 + 3y_1^2}$ — the same as 1).

$\boxed{\text{225 Problems in NT}}$

$p = a^2 + ab + b^2 \iff p = 3$ or $p = 1 \bmod 3$

$p = a^2 + b^2 \iff p = 4k+1$ or $p = 2$