Chapter 2

Date: Feb 23 Made by Eric

Definitions and Theorems

Definition 1. *Let* $p \in \mathbb{N}$. p *is a prime if* $\forall a \in \mathbb{N}, a|p \implies a = 1$ *or* p

Theorem 1. *Let* $f(x) = a_0 + a_1x + \cdots + a_kx^k$. *If there exists prime number* p*, such* $p^2 \nmid a_0$ *and* $p|a_i, \forall 0 \leq i \leq k-1$*, and* $p \nmid a_k$*,* $f(x)$ *is irreducible.*

Proof. Assume there exists two non-constant integer polynomials $g(x), h(x) \in \mathbb{Z}[x]$, such $f(x) = g(x)h(x) = (b_0 + b_1x + \cdots + b_nx^n)(c_0 + c_1x + \cdots + c_mx^m)$, where $deg(g) \leq deg(h)$

$p|a_0$ and $p^2 \nmid a_0 \implies (p|b_0$ and $p \nmid c_0)$ or $(p|c_0$ and $p \nmid b_0)$.

Case: $(p|b_0$ and $p \nmid c_0)$

$a_1 = b_1c_0 + b_0c_1$ and $p|b_0$ and $p \nmid c_0$ and $p|a_1 \implies p|b_1$

We claim $p|b_i, \forall 0 \leq i \leq n$

We use induction to prove it.

Base step: $p|b_0$

$p|b_0$ is the premise.

Induction step: $p|b_i, \forall 0 \leq i \leq u \longrightarrow p|b^{u+1}$

Given $p|b_i, \forall 0 \leq i \leq u$.

$a_{u+1} = b_0c_{u+1} + \sum_{i=1}^{u+1} b_ic_{u+1-i}$ and $p \nmid c_0 \implies p|b^{u+1}$ OCIP

$a_k = b_nc_m \implies p|a_k$, CaC OPID

Case: $(p|c_0 \text{ and } p \not| b_0)$

We claim $p|c_i, \forall 0 \leq i \leq m$

Base step: $p|c_0$

$p|c_0$ is the premise.

Induction step:$p|c_i, \forall 0 \leq i \leq u \implies p|c_{u+1}$

$a_{u+1} = c_{u+1}b_0 + \sum_{i=1}^{n} b_i c_{u+1-i}$ and $p \not| b_0 \implies p|c_{u+1}$ OCIP

$a_k = b_n c_m \implies p|a_k$, CaC OPID

■

Theorem 2. *Let $p \in \mathbb{Z}$ be a prime, and $a, b \in \mathbb{Z}$.*

(i): $p|a$ or $gcd(p,a) = 1$

(ii): $p|ab \implies p|a$ or $p|b$

Proof. (i)

$gcd(p,a)|p$ by definition.

p is a prime $\implies gcd(p,a) = 1$ or $gcd(p,a) = p$

If $gcd(p,a) = 1$ OPID

If $gcd(p,a) = p$, $gcd(p,a)|a \implies p|a$ OPID

(ii)

WOLG, assume $p \not| a$

$gcd(p,a) = 1$ by (i).

$\exists \alpha, \beta \in \mathbb{Z}, \alpha p + \beta a = 1 \implies \alpha pb + \beta ab = b$

$p|ab \implies p|\alpha pb + \beta ab = b$ ■

Theorem 3. *There are infinitely many prime.*

Proof. Assume there are only finitely k many primes $\{p_1, \dots, p_k\}$

By Fundamental theorem of Arithmetic, $\exists 1 \leq j \leq k, p_j | (\Pi_{i=1}^k p_i) + 1$

$\forall 1 \leq j \leq k, \Pi_{i=1}^k p_i = qp + 1, \exists q \in \mathbb{Z} \implies p_j \not| \Pi_{i=1}^k p_i$ CaC ■

Theorem 4. *The n-th prime p_n satisfy $p_n \leq 2^{2^{n-1}}$*

Proof. We prove by induction.

Base step: The first prime p_1 satisfy $p_1 \leq 2^{2^{1-1}}$

$p_1 = 2 \leq 2 = 2^{2^{1-1}}$

Induction step: $\forall 1 \leq i \leq n, p_i \leq 2^{2^{n-1}} \implies p_{n+1} \leq 2^{2^{n+1-1}}$

By the fundamental theorem of arithmetic, there exists a prime number p_k, such $p_k | (\Pi_{i=1}^n p_i) + 1$

$\forall 1 \leq i \leq n, p_i \not| (\Pi_{i=1}^n p_i) + 1 \implies p_k \neq p_i \implies k > n \implies p_{n+1} \leq p_k \leq (\Pi_{i=1}^n p_i) + 1$

$\forall 1 \leq i \leq n, p_i \leq 2^{2^{n-1}} \implies p_{n+1} \leq p_k \leq (\Pi_{i=1}^n p_i) + 1 \leq \Pi_{i=1}^n 2^{2^{i-1}} + 1 = 2^{(\sum_{i=1}^n 2^{i-1})} + 1 = 2^{2^n - 1} + 1 = \frac{1}{2} 2^{2^n} + 1 \leq 2^{2^{n+1-1}}$ ■

Theorem 5. *There are infinitely many primes of the form $4u + 3, \exists u \in \mathbb{N}$*

Proof. Assume there are finitely n number amount of primes $\{p_1, \dots, p_n\}$ of the form $4u_i + 3, \exists u_i \in \mathbb{N}$

$(4u_1 + 3) \dots (4u_n + 3) = 4q + 1$ or $4q + 3, \exists q \in \mathbb{N}$

Case: $(4u_1 + 3) \dots (4u_n + 3) = 4q + 1$

$4q+3 = (4q+1)+2 = (4u_1+3) \dots (4u_n+3)+2 \implies \forall u_i \in u_I, 4u_i+3 \not| 4q+3$

Do prime factorization on $4q + 3$, and classify all the primes from the result, we see it contains no prime of the form $4u_i + 3$, so it contains only primes of the form $4k + 1$ or $4k$ or $4k + 2$

It contains no prime of the form $4k$ nor prime of the form $4k + 2$, since $4q + 3$ is odd.

So, $4q + 3 = (4k_1 + 1) \dots (4k_m + 1)$

$4q + 3 \equiv 3 \not\equiv 1 \equiv (4k_1 + 1) \dots (4k_m + 1) \pmod 4$ CaC

$$\text{Case: } (4u_1+3)\dots(4u_n+3) = 4q+3$$

$4(q+1)+3 = 4q+7 = (4u_1+3)\dots(4u_n+3)+4$

$\implies \forall u_i \in u_I, 4u_i+3 \nmid 4q+7$

Do prime factorization on $4(q+1)+3$, and classify all the primes from the result, we see it contains no prime of the form $4u_i+3$, so it contains only primes of the form $4k+1$ or $4k$ or $4k+2$

It contains no prime of the form $4k$ nor prime of the form $4k+2$, since $4q+3$ is odd.

So, $4q+7 = (4k_1+1)\dots(4k_m+1)$

$4q+7 \equiv 3 \not\equiv 1 \equiv (4k_1+1)\dots(4k_m+1)$ (mod 4) CaC

∎

Theorem 6. 2^m+1 *is a prime* $\implies \exists 0 \le n, m = 2^n$

Proof. Assume m is not a power of 2

We **claim (i)** there exists $0 \le p$ and odd natural number q, such $m = 2^p q$

We prove by induction. (In the rest of the whole proof, q denote an odd number)

$$\text{Base step: } 2|m \text{ or } m = 2^p q$$

$2 \nmid m \implies m = 2^0 m = 2^0 q$

$$\text{Induction step: } 2^k|m \text{ or } m = 2^p q \implies 2^{k+1}|m \text{ or } m = 2^p q$$

$2^k|m \implies m = 2^k r$

If r is odd, $r = q \implies m = 2^k q$

If r is even, $m = 2^k r = 2^{k+1}\frac{r}{2} \implies 2^{k+1}|m$

OCIP

From **claim (i)** $m = 2^p q$

So $2^m+1 = 2^{(2^p)q}+1 = [2^{(2^p)}]^q+1$

Notice $2^{(2^p)}+1|[2^{(2^p)}]^q+1$, since $\forall x \in \mathbb{Z}, x+1|x^q+1$ (for instance $x+1|x^3+1$)

So $2^{2^p}+1|[2^{(2^p)}]^q+1 = 2^m+1$ CaC

∎

Definition 2. *A Fermat's number* F_n *is* $2^{2^n}+1$

Lemma 7. *Distinct Fermat's numbers are coprime.*

Proof. Let $2^{2^n}+1$ and $2^{2^{n+k}}+1$ be two distinct Fermat's number.

$2^{2^{n+k}} = 2^{2^n 2^k} = (2^{2^n})^{2^k}$

$2^{2^n}+1 | (2^{2^n})^{2^k} - 1$, since $\forall x \in \mathbb{Z}, x+1 | x^{2q} - 1$ (recall in Algebra, how we reduce polynomial. This should be familiar to you)

Let $a = 2^{2^n}+1, b = 2^{2^{n+k}}+1$

From above, we have $a|b-2$

So $b-2 = ca, \exists c \in \mathbb{Z}$

So $b = ca+2$

Clearly, $gcd(b = ca+2, a) = 2$ or 1.

$2 \not| 2^{2^n}+1 = a \implies gcd(b = ca+2, a) = 1 \implies gcd(2^{2^n}+1, 2^{2^{n+k}}+1) = 1$

■

Theorem 8. $m > 1$ *and* $a^m - 1$ *is a prime* $\implies a = 2$ *and* m *is a prime.*

Proof. $\forall a \in \mathbb{N}, a-1 | a^m - 1 \implies a = 2$

Assume m is not a prime.

$\exists 1 < p, q \in \mathbb{N}, m = pq$

$a^m - 1 = a^{pq} - 1 = (a^p)^q - 1$

$a^p - 1 | (a^p)^q - 1$ CaC

■

Exercises

2.6

2.6(a)

Proof. By division algorithm, every prime is either of the form of $3q$ or $3q+1$ or $3q+2$

If a prime p is of the form $3q$, then $3|p$

So $p = 3$ CaC

So every prime p is either of the form of $3q+1$ or $3q+2$

■

2.6(b)

Proof. Assume there exists only finitely n amount of primes $\{3u_1+2, \cdots, 3u_n+2\}$

$(3u_1+2)\dots(3u_n+2)$ is either of the form $3k+1$ or $3k+2$

$$\text{Case: } (3u_1+2)\dots(3u_n+2) = 3k+1, \exists k \in \mathbb{N}$$

$3k+2 = (3u_1+2)\dots(3u_n+2)+1 \implies \forall 1 \le i \le n, 3u_i+2 \nmid 3k+2$

Do prime factorization on $3k+2$, and classify all the primes from the result, we see it contains no prime of the form $3q+2$, so it contains only primes of the form $3q+1$ or $3q$

Clearly, $3q \nmid 3k+2$

So, $3k+2 = (3k_1+1)\dots(3k_m+1)$

$3k+2 \equiv 2 \not\equiv 1 \equiv (3k_1+1)\dots(3k_m+1) \pmod 3$ CaC

$$\text{Case: } (3u_1+2)\dots(3u_n+2) = 3k+2, \exists k \in \mathbb{N}$$

$3k+5 = (3u_1+2)\dots(3u_n+2)+3 \implies \forall 1 \le i \le n, 3u_i+2 \nmid 3k+5$

Do prime factorization on $3k+5$, and classify all the primes from the result, we see it contains no prime of the form $3q+2$, so it contains only primes of the form $3q+1$ or $3q$

Clearly, $3q \nmid 3k+2$

So, $3k+5 = (3k_1+1)\dots(3k_m+1)$

$3k+5 \equiv 2 \not\equiv 1 \equiv (3k_1+1)\dots(3k_m+1) \pmod 3$ CaC ■

2.7

Proof. We shows $(k+1)!+2, (k+1)!+3, \cdots, (k+1)!+(k+1)$ is a solution.

Obviously, $(k+1)!+2, (k+1)!+3, \cdots, (k+1)!+(k+1)$ is a sequence of k integer.

We claim $(k+1)!+2, (k+1)!+3, \cdots, (k+1)!+(k+1)$ are all composite numbers.

$\forall 2 \leq i \leq k+1, (k+1)! + i = [(\Pi_{j=1, j\neq i}^{k+1} j) + 1]i$

OCIP OPID

■

2.9

Proof. Assume a is odd.

a^m is odd $\implies a^m + 1$ is even $\implies 2|a^m + 1$ CaC

Assume m is not a power of 2

So $m = 2^p q, \exists p \in \mathbb{Z}^+, \exists q$ is an odd number.

$a^m + 1 = a^{2^p q} + 1 = (a^{2^p})^q + 1 \implies a^{2^p} + 1|(a^{2^p})^q + 1 = a^m + 1$ CaC

■

2.17

Proof. 3 is a prime and $11 = 3^2 + 2$ is also a prime. ■

2.18

Proof. $\forall 2 \leq i \leq p-1, i \not| (p-1)! + 1$

Assume p is not a prime.

$\exists 2 \leq u \leq p-1, u|p$

$p|(p-1)! + 1 \implies u|(p-1)! + 1$ CaC

■