Number Theory 2

November 19, 2019

1 Euclidean Algorithm

Let $a, b \in \mathbb{N}\backslash\{0\}$ with $b < a$. Recursively define

$$F_{a,b}(n+2) = \begin{cases} 0 & \text{if } F_{a,b}(n+1) = 0 \\ r & \text{if } F_{a,b}(n) = qF_{a,b}(n+1) + r \quad (0 \leqslant r < F_{a,b}(n+1)) \end{cases}$$

1.1 Properties

Let $a, b, n \in \mathbb{N}\backslash\{0\}$ with $b < a$. If $F_{a,b}(n) \neq 0$, then $F_{a,b}(n+1) < F_{a,b}(n)$.

Let $a, b, n \in \mathbb{N}\backslash\{0\}$ with $b < a$. If $F_{a,b}(n) = 0$, then for all $m \geqslant n$, $F_{a,b}(m) = 0$.

Let $a, b \in \mathbb{N}\backslash\{0\}$ with $b < a$. There exists $n \in \mathbb{N}$ such $F_{a,b}(n) = 0$.

Let $a, b \in \mathbb{N}\backslash\{0\}$ with $b < a$ and let $n \in \mathbb{N}$. If $F_{a,b}(n) \neq 0$, then $\gcd(a,b) = \gcd(F_{a,b}(n), F_{a,b}(n+1))$.

Let $a, b \in \mathbb{N}\backslash\{0\}$ with $b < a$. Let $n_0 \geqslant 2$ be least such that $F_{a,b}(n_0) = 0$. Then $\gcd(a,b) = F_{a,b}(n_0 - 1)$.

1.2 Exercise

Calculate gcd(124, 16).

Solve the Diophantine Equation $124x + 16y = \gcd(124, 16)$.

Find the inverse of $[9]_{124}$ in the group $(\mathbb{Z}/124\mathbb{Z})^*$.

2 Diophantine Equations

2.1 Theorems

Let $a, b, c \in \mathbb{Z}$. There exists a solution to the linear Diophantine equation $ax + by = c$ if and only if $\gcd(a,b)|c$.

Let $a, b, c, d \in \mathbb{Z}$ with $d = \gcd(a,b)$ and $d|c$. Let (x_0, y_0) be a solution to $ax + by = c$. For all $t \in \mathbb{Z}$, (x_t, y_t) is a solution to $ax + by = c$ where

$$x_t = x_0 + \frac{b}{d}t \text{ and } y_t = y_0 - \frac{a}{d}t$$

Moreover, if (x', y') is a solution to $ax + by = c$, then there exists a $t \in \mathbb{Z}$ such that $(x', y') = (x_t, y_t)$.

2.2 Exercise

Solve the Diophantine Equation $172x + 20y = 1000$.

3 Chinese Remainder Theorem

Let $m_1, ..., m_n \in \mathbb{N}\backslash\{0\}$ be pairwise relatively prime and let $a_1, ..., a_n \in \mathbb{Z}$. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 (\text{mod } m_1) \\ x &\equiv a_2 (\text{mod } m_2) \\ &\cdots \\ x &\equiv a_n (\text{mod } m_n) \end{aligned}$$

has a unique solution (mod m) where $m = m_1 \cdots m_n$.

3.1 Proof

First we can find a solution of the system of congruences.

$$x \equiv M_1 M_1^{-1} a_1 + \cdots + M_n M_n^{-1} a_n$$

where $M_k = \frac{m}{m_k}$, and $M_k M_k^{-1} \equiv 1(\text{mod } m_k)$.
Since gcd(M_k, m_k)=1, then M_k^{-1} exists for every $1 \leqslant k \leqslant n$. ($[M_k]_{m_k} \in (\mathbb{Z}/m_k\mathbb{Z})^*$)
Since $m_k | M_t$ if $k \neq t$, then $x \equiv M_k M_k^{-1} a_k \equiv a_k(\text{mod } m_k)$.

Now we need to show the uniqueness of the solution. If there exists another solution x', then $m_k | (x' - x)$ for all $1 \leqslant k \leqslant n$. Since $m_1, ..., m_n \in \mathbb{N}\backslash\{0\}$ are pairwise relatively prime, then $m | (x' - x)$, which means $x' \equiv x(\text{mod } m)$.

3.2 Exercise

Find the minimum $x \in \mathbb{Z}^+$ such that

$$\begin{aligned} x &\equiv 2(\text{mod } 3) \\ x &\equiv 3(\text{mod } 5) \\ x &\equiv 2(\text{mod } 7) \end{aligned}$$

Find the minimum $x \in \mathbb{Z}^+$ such that $43x \equiv 12(\text{mod } 56)$.

4 Wilsons Theorem

Let $p \in \mathbb{N}$ be prime. Then $(p-1)! \equiv -1 (\text{mod } p)$.

Proof. The main idea of the proof is finding the inverse.

1. For all $1 \leqslant x \leqslant p-1$, there exists $1 \leqslant x^{-1} \leqslant p-1$ such that $xx^{-1} \equiv 1 (\text{mod } p)$. (Why?)

2. The inverse of x is unique. I.e. $1 \leqslant x^{-1} \leqslant p-1$ is unique for all $1 \leqslant x \leqslant p-1$. (Why?)

3. However x and x^{-1} are not always different. Find the solution of $x^2 \equiv 1 (\text{mod p})$. (The answer is $x = 1, p-1$.)

4. We can conclude that $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 (\text{mod } p)$

4.1 Another Proof for Wilsons Theorem

Consider the following equations

$$\begin{aligned}
x^{p-1} - 1 &= (x-1)f_1(x) + C_1 \\
f_1(x) &= (x-2)f_2(x) + C_2 \\
\cdots &= \cdots \\
f_{k-1}(x) &= (x-k)f_k(x) + C_k \\
\cdots &= \cdots \\
f_{p-2}(x) &= (x-(p-1))f_{p-1}(x) + C_{p-1} \\
f_{p-1}(x) &= 1 (\text{Why?})
\end{aligned}$$

where $C_1, C_2, \cdots, C_{p-1}$ are all numbers. ($C_1, \cdots, C_{p-1}$ do not change with x.)
Now, you need to prove $p | f_m(n)$ when $m < n$. Then $p | C_k$ for all $1 \leqslant k \leqslant p-1$. (Prove it yourself. It requires Format's Little Theorem.)
Therefore,

$$x^{p-1} - 1 \equiv (x-1)f_1(x) \equiv (x-1)(x-2)f_2(x) \equiv \cdots \equiv (x-1)\cdots(x-(p-1)) \pmod p$$

Let $x = p$. This can be converted into $(p-1)! \equiv -1 \pmod p$

5 Exercise

1. Show that there exists infinite tuples of successive positive integers p, q, r, such that there exists p_1, q_1, r_1, and $x \equiv 1 \pmod{x_1^3}$ $(x = p, q, r)$

2. Let $m, n \in \mathbb{Z}^+$. For all $k \in \mathbb{N}$, $\gcd(11k-1, m)$=$\gcd(11k-1, n)$. Show that there exists $l \in \mathbb{Z}$, such that $m = 11^l n$. (Hint. Try to find $p \in \mathbb{Z}^+$ where p is not a multiple of 11, such that $p|m$ and $p \nmid n$.)

3. Let $a, b, c, d \in \mathbb{Z}^+$, and $\gcd(a, b, c, d)$=1.For all $n \in \mathbb{Z}^+$, $\gcd(an+b, cn+d) = 1$. Show that for any prime $p|ad-bc$, a and c are also multiples of p.

6 Quadratic Remainder

Let p be prime and $p > 2$. Let $d \in \mathbb{Z}^+$ and $\gcd(p, d) = 1$. Show that
(i)The congruence $x^2 \equiv d(\text{mod } p)$ has at least one solution if and only if $d^{(p-1)/2} \equiv 1 \pmod{p}$.
(ii)The congruence $x^2 \equiv d(\text{mod } p)$ has no solution if and only if $d^{(p-1)/2} \equiv -1 \pmod{p}$.