Number Theory 4

03 September 2023 11:20

Bézout's Theorem:-

Let a, b be integers. Then the equation $ax+by=n$ has a solution if and only if $\gcd(a,b) \mid n$. $(x, y \in \mathbb{Z})$

Proof:- $a = gq_1$ $b = gq_2$ $\gcd(q_1, q_2) = 1$ $\Rightarrow g \mid n$

$g \mid n \Rightarrow n = gk_1$, $g = \gcd(a,b) \Rightarrow a = gq_1$, $b = gq_2$

To prove:- $\exists x, y$ such that, $gq_1 x + gq_2 y = gk_1 = n$

Hint:- $\exists x_0, y_0$ such that $\boxed{ax_0+by_0 = g}$ $\Rightarrow ak_1x_0 + bk_1y_0 = gk_1$
$\Rightarrow ax+by = gk_1$

This proof:- $a = gq_1$ $b = gq_2$
gq_1x_0 $gq_2y_0 = g$ $\Rightarrow (q_1x_0 + q_2y_0) = 1$

Idea:-
WLOG
$q_1 > q_2 \Rightarrow q_1 = q_2m_1 + r_1$ $q_1 - q_2m_1$, q_2 are coprime
$0 \le r_1 < q_2$

$q_2 = r_1m_2 + r_2$, $q_1 - q_2m$, $q_2 - r_1m_2$ are coprime

So the values are decreasing. So one will reach 1 in some steps

$q_1x_0 + q_2y_0 = m \Rightarrow 1 \mid m$

Rigorous Proof of Bezout's Theorem.- $S = \{ax+by > 0 : a, b \in \mathbb{Z}\}$ and g be the minimum of S.

Suppose g doesn't divides $a \Rightarrow a = qg + r$ $0 < r < g$ and $q \geq 0$

$a = gq + r$, $gq = a - r$

$g = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$

$(ax_0 + by_0)q = a - r \Rightarrow r = a - aqx_0 - bqy_0 = a(1-qx_0) + bqy_0$

So r is a linear combination of a and b

$\Rightarrow r \in S \Rightarrow r \geq g$ but we took $r < g$ Contradiction

Thus $g \mid a$. Similarly $g \mid b$

$a = dc$, $b = ec$, $g = ax_0 + by_0 = c(dx_0 + ey_0) \Rightarrow c \mid g$

minimum of this is g

$\Rightarrow$ any common divisor of a, b is dividing g

$\to$ minimum of this is g

$\Rightarrow$ any common divisor of a, b is dividing g

$\Rightarrow g$ is $\gcd(a, b)$

$ax_0 + by_0 = g$ exists for some $x_0, y_0 \in \mathbb{Z}$

Thus Bezout's Theorem is proved

Euclid's Lemma:- If $c|ab$ and $\gcd(a,c) = 1$, then $c|b$.

Proof:- Algebraic:- $c|ab$, $\gcd(a,c)=1$, $ab = ck \Rightarrow b = ck_1$, $a = k_2$

we can write it as $ab = ck_1k_2 = ck$

Set theoretic:- $c|ab \Rightarrow C \subset (A+B)$

$\gcd(a,c) = 1 \Rightarrow C \cap A = \phi$

So, $C \subset B \Rightarrow c|b$

By using Bezout's Lemma:- (Homework)

HW:- (Putnam 2000) Prove the expression $\dfrac{\gcd(m,n)}{n}\dbinom{n}{m}$ is an integer for all pairs of integers $n \geq m \geq 1$

$\gcd(a,c)=1$, $ax + cy = n \Rightarrow ax + cy = 1$ exists

$bax + bcy = b \Rightarrow cby = b - abx$

$\Rightarrow cby = b(1 - ax) \Rightarrow ck = b(1-ax)$

$cby + abx = b$, $c|cby$ & $c|ab \Rightarrow c|abx$

$\Rightarrow c\,|(cby + abx) \Rightarrow c|b$

Case 1

$n = m$, $\gcd(n,m) = m = n$

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = \left(\frac{M}{n}\right)\frac{n!}{(n-m)!\,m!} = \frac{n!}{n!} = 1$$

Case 2:- $n > m$

$\gcd(m,n) = d$, $m = dk_1$, $n = dk_2$, $\gcd(k_1,k_2) = 1$

$$\frac{d}{n}\left(\frac{n!}{(n-m)!\,m!}\right) = \frac{(n-1)(n-2)\dots(n-m+1)}{k_1\,(m-1)!}$$

$$\frac{d}{n}\left(\frac{n!}{(n-m)!\,m!}\right) = \frac{\qquad}{k_1 (m-1)!}$$

$\frac{d}{n}\binom{n}{m}$ $\quad\binom{n}{m}$ is an integers. Now we have to show that $\binom{n}{m}$ has a factor k_2

$= \frac{1}{k_2}\binom{n}{m}$

$$\frac{n!}{(n-m)!\,m!} = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!} = \frac{k_2 d\,(n-1)(n-2)\cdots(n-m+1)}{m!}$$

$$= \frac{k_2 d}{k_1 d}\,\frac{(n-1)\cdots(n-m+1)\,(n-m)!}{(m-1)!\,(n-m)!}$$

both are integers

$$= \frac{k_2}{k_1}\binom{n-1}{m-1}! = k_2 C$$

k_1, k_2 are coprime

so, $\binom{n-1}{m-1}!$ must have factor k_1 for $\binom{n}{m}$ to be integer

$\frac{1}{k_1}\binom{n-1}{m-1}$ is integer, let it be C

$$\frac{d}{n} k_2 C = C \in \mathbb{Z}$$

$$\Rightarrow \frac{\gcd(n,m)}{n}\binom{n}{m} \text{ is integer}$$

Home-Work :- Prove this Putnam 2000 question using Bezout's idea

---

Base System :-

$$6154 = 6\times 10^3 + 1\times 10^2 + 5\times 10^1 + 4\times 10^0$$

In decimal, $a_n \cdots a_3 a_2 a_1 a_0 = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$

$a_i \in \{0, \ldots, 9\}$

In binary, $a_i \in \{0, 1\}$

$$a_n a_{n-1} \cdots a_2 a_1 a_0 = a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_2 2^2 + a_1 2 + a_0$$

$$10110 = 1\times 2^4 + 0\times 2^3 + 1\times 2^2 + 1\times 2 + 0 = 16 + 0 + 4 + 2 = 22$$

Base k, $a_i \in \{0, \ldots, k-1\}$

$$a_n a_{n-1} \cdots a_1 a_0 = a_n k^n + a_{n-1} k^{n-1} + \cdots + a_1 k + a_0 k^0$$

Proposition:- $a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_1 2 + a_0 < 2^{n+1}$, $a_i \in \{0,1\}$ $\rightarrow$ Claim $\forall n \in \mathbb{Z}$

Base case :- For $n = 0$, $\quad a_0 < 2^1$ as $a_0 \in \{0, 1\}$

Inductive Assumption :- for $n = m$ it is true for $m \geq 0 \Rightarrow \underbrace{a_m 2^m + \cdots + a_1 m + a_0}_{K\ (\text{let})} < 2^{m+1}$

Inductive Step :- For $n = m+1$, $\qquad K < 2^{m+1}$

Inductive Assumption:

Inductive Step:- For $n = m+1$,

$$a_{m+1}2^{m+1} + a_m 2^m + \cdots + a_0 = a_{m+1}2^{m+1} + k \qquad k < 2^{m+1}$$

$$< \left(a_{m+1}2^{m+1} + 2^{m+1}\right)$$

Now we know $a_{m+1} \in \{0, 1\}$

$\Rightarrow a_{m+1} \leq 1$

$\Rightarrow a_{m+1} + 1 \leq 2$

$$\Rightarrow a_{m+1}2^{m+1} + k < 2^{m+1}(a_{m+1} + 1)$$

$$\leq 2^{m+1}(2)$$

$$= 2^{m+2}$$

$$\Rightarrow a_{m+1}2^{m+1} + k < 2^{m+2}$$

Hence our assumption is correct

Hence claim is true

2^k looks like $100\cdots0$ in base 2

Q> Prove that any number of the form

Ans:- (HomeWork) try to use previous ideas

$$(10010)_2 \times 2 = (100100)_2 = (10010)_2 \times (10)_2$$

$9 \times 10 = 90$

$19 \times 10 = 190$

$$(1001)_2 \times 2 = (10010)_2$$

$$(10)_2 = 2$$

$$(a_n 2^n + \cdots + a_1 2 + a_0) \times 2 = a_n 2^{n+1} + \cdots + a_1 2^2 + a_0 2^1 + 0$$

$$= (a_n a_{n-1} \cdots a_0 0)_2$$

$k = (10)_k$

$$(a_n a_{n-1} \cdots a_1 a_0)_k \times k = (a_n a_{n-1} \cdots a_1 a_0 0)_k$$

$1k^1 + 0 = 1$

HomeWork

Q> Any number N has a unique representation $(a_n a_{n-1} \cdots a_0)_k$ in base k.

for $a_i \in \{0, \ldots, k-1\}$

Theorem in ONT:-

For natural numbers a, m, n, we have $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$

Ans:- Hint is in ONT book page 12.

Do the full proof (HomeWork)

$$(a_n a_{n-1} \cdots a_1 a_0)_k + (b_n b_{n-1} \cdots b_1 b_0)_k = (?)_k$$

| $91 + 22 = 113$

$(a_n a_{n-1} \cdots a_1 a_0)_k + (b_n b_{n-1} \cdots b_1 b_0)_k = (?)_k$

$< 2^{n+1}$ $\quad < 2^{n+1}$ $\quad < 2^{n+2}$

$= a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_1 2 + a_0$
$+ b_n 2^n + b_{n-1} 2^{n-1} + \cdots + b_1 2 + b_0$

$= (a_n + b_n) 2^n + (a_{n-1} + b_{n-1}) 2^{n-1} + \cdots + (a_0 + b_0)$

To have it in base k we must it in the form $(c_{n+1} c_n c_{n-1} \cdots c_1 c_0)_k$
where $c_i \in \{0, \ldots, k-1\}$

$$\Rightarrow \quad c_0 = (a_0 + b_0) \bmod k$$

$$c_1 = (\underbrace{a_1 + b_1 + \lfloor (a_0 + b_0)/k \rfloor}_{M_1}) \bmod k$$

$$c_2 = (\underbrace{a_2 + b_2 + \lfloor M_1/k \rfloor}_{M_2}) \bmod k$$

$$\vdots$$

$$c_n = (\underbrace{a_n + b_n + \lfloor M_{n-1}/k \rfloor}_{M_n}) \bmod k$$

$$c_{n+1} = \lfloor M_n/k \rfloor$$

$91 + 22 = 113$

$\begin{array}{r} 199 \\ 233 \\ \hline 432 \end{array}$

$\begin{array}{r} 92 \\ 13 \\ \hline 105 \end{array}$

$\lfloor 12/10 \rfloor = 1$