



Discrete Structures

Number Theory



Division

Definition:

- $a \mid b$ iff $\exists c: b = ac$
- a divides b , b is a multiple of a , a is a factor of b
- If a does not divide b , we write $a \nmid b$

Properties:

1. $a \mid b, b \mid c \rightarrow a \mid c$
2. $a \mid b, a \mid c \rightarrow a \mid bx + cy$
3. $a \mid b, b \mid a \leftrightarrow |a| = |b|$
4. $a \mid 1 \leftrightarrow |a| = 1$
5. $a \mid b \rightarrow a \mid bc$
6. $\forall n \geq 1: a \mid b \leftrightarrow a^n \mid b^n$

Some Proofs

Proof (2):

$$a|b, a|c \rightarrow \exists b', c': b = ab', c = ac' \rightarrow bx = ab'x, cy = ac'y \\ \rightarrow bx + cy = a(b'x + c'y) \rightarrow a|bx + cy$$

Proof (6):

$$a|b \rightarrow \exists c: b = ac \rightarrow b^n = a^n c^n \rightarrow a^n|b^n$$

The reverse is not simple now; wait for GCD.

Some Problems

Problem:

if $x_1x_2 + x_2x_3 + \cdots + x_nx_1 = 0$ and $x_i \in \{1, -1\}$, then $4|n$

Solution:

It is clear $2|n$. So, $n/2$ terms are $+1$ and $n/2$ terms -1

Multiply all terms. In one hand we have $(-1)^{n/2}$. In the other hand we have $(x_1x_2x_3 \dots x_n)^2 = 1$. Then

$$(-1)^{n/2} = 1 \rightarrow 4|n$$

Problem:

$$a - c \mid ab + cd \rightarrow a - c \mid ad + bc$$

Solution:

$$a - c \mid (ad + bc) - (ab + cd) = (a - c)(d - b)$$

Some Problems

Problem: $13|4^{2n+1} + 3^{n+2}$

Solution:

- Basis Step: $13|4^1 + 3^2$

- Inductive Step:

$$13|4^{2n+1} + 3^{n+2} \rightarrow 13|4^{2(n+1)+1} + 3^{(n+1)+2}$$

$$\begin{aligned} & (4^{2(n+1)+1} + 3^{(n+1)+2}) - (4^{2n+1} + 3^{n+2}) \\ &= 15 \times 4^{2n+1} + 2 \times 3^{n+2} = 13 \times 4^{2n+1} + 2(4^{2n+1} + 3^{n+2}) \end{aligned}$$

Problem: $9|a^2 + ab + b^2 \rightarrow 3|a, 3|b$

Solution:

$$\begin{aligned} 9|a^2 + ab + b^2 &= (a - b)^2 + 3ab \rightarrow 3|a - b \\ &\rightarrow 9|(a - b)^2 \rightarrow 9|3ab \rightarrow 3|a \vee 3|b \\ (3|a - b) \wedge (3|a \vee 3|b) &\rightarrow 3|a \wedge 3|b \end{aligned}$$

Greatest Common Divisor

Definition:

$GCD(a, b) = d$ iff

1. $d|a, d|b$
2. $\forall d': d'|a, d'|b \rightarrow d' \leq d$

Properties (Let 's denote $GCD(a, b)$ by (a, b)):

1. $(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b)$
2. $\forall k: (a, b) = (a, b + ak)$
3. $\exists x, y: ax + by = (a, b)$
4. $(a, b) = (a, c) = 1 \rightarrow (a, bc) = 1$
5. $(a^n, b^n) = (a, b)^n$
6. $a|bc, (a, b) = 1 \rightarrow a|c$
7. $(ka, kb) = |k|(a, b)$
8. $a|c, b|c, (a, b) = 1 \rightarrow ab|c$

Some Proofs

Proof (2)

Let $(a, b) = d$, $(a, b + ak) = d'$

$(a, b) = d \rightarrow d|a, d|b \rightarrow d|a, d|b + ak \rightarrow d \leq d'$

Similarly $d' \leq d$, and then $d = d'$

Proof (6)

$(a, b) = 1 \rightarrow \exists x, y: ax + by = 1 \rightarrow acx + bcy = c$
 $\rightarrow acx + aa'y = c \rightarrow a(cx + a'y) = c \rightarrow a|c$

Proof (8)

$(a, b) = 1 \rightarrow \exists x, y: ax + by = 1 \rightarrow acx + bcy = c$
 $\rightarrow abb'x + baa'y = c \rightarrow ab(b'x + a'y) = c \rightarrow ab|c$

Some Problems

Problem: show $(3n + 2, 7n + 5) = 1$

Solution 1:

$$(3n + 2, 7n + 5) = d \rightarrow d|3n + 2, d|7n + 5 \rightarrow d|7(3n + 2) - 3(7n + 5) = -1 \rightarrow d = 1$$

Solution 2:

$$\begin{aligned}(3n + 2, 7n + 5) &= (3n + 2, 7n + 5 - 2(3n + 2)) \\ &= (3n + 2, n + 1) = (n + 1, 3n + 2) \\ &= (n + 1, 3n + 2 - 3(n + 1)) = (n + 1, -1) = 1\end{aligned}$$

Problem: $a | b \leftrightarrow a^n | a^n$

Solution: $a^n | b^n \rightarrow (a^n, b^n) = a^n \rightarrow (a, b) = a \rightarrow a | b$

Some Problems

Definition:

if $(a, b) = 1$, they are called relatively prime

Problem: Among 5 consecutive numbers, there is one which is relatively prime to the other four numbers

Solution:

for any $|a - b| < 5$, we know $(a, b) = 1, 2, 3$, or 4

It suffices to show there is a number x s.t. $(x, 6) = 1$

Between 5 consecutive numbers, there are two consecutive odd numbers. One of these two is not divisible by 3; otherwise their difference which is 2 must be divisible by 3. This number is the answer.

Problem: Prove problem for 16 consecutive numbers

Least Common Multiples

Definition:

- $LCM(a, b) = L$ iff
 1. $L > 0$
 2. $a|L, b|L$
 3. $\forall L': a|L', b|L' \rightarrow L \leq L'$

Properties (Let $[a, b]$ denote $LCM(a, b)$):

1. $[a, b] = [b, a] = [-a, b] = [a, -b] = [-a, -b]$
2. $[a^n, b^n] = [a, b]^n$
3. $[ka, kb] = |k|[a, b]$
4. $[a, b] = |ab|/(a, b)$

Some Problems

Problem: $[a, b, c] = \frac{abc}{(ab, ac, bc)}$

Solution:

$$\begin{aligned} [a, b, c] &= [[a, b], c] = \left[\frac{ab}{(a, b)}, c \right] = \frac{\frac{abc}{(a, b)}}{\left(\frac{ab}{(a, b)}, c \right)} \\ &= \frac{\frac{abc}{(a, b)}}{\frac{(ab, ac, bc)}{(a, b)}} = \frac{abc}{(ab, ac, bc)} \end{aligned}$$

Division Algorithm

Theorem:

$$\forall a, b \neq 0 \exists q, r: a = bq + r, 0 \leq r < |b|$$

Proof:

- For simplicity assume $a, b > 0$
- Consider $R = \{a - bq \mid a - bq \geq 0\}$
- R has a least element; called it r ; $r = a - bq$ for some q
- r must be smaller than b , otherwise
- $0 \leq r - b = a - bq - b = a - b(q + 1) \rightarrow r - b \in R$

Some Problems

Any number can be written in any of the following format

- $2k, 2k + 1$
- $3k, 3k + 1, 3k + 2$
- $4k, 4k + 1, 4k + 2, 4k + 3,$
- ...

Problem: show $120|n^5 - n$ for odd n

Solution:

$$3 \times 5 \times 8 | n(n-1)(n+1)(n^2+1)$$

We know $3|n(n-1)(n+1)$

$$5 \nmid n(n-1)(n+1) \rightarrow n = 5k \mp 2 \rightarrow 5|n^2 + 1$$

$$n = 2k + 1 \rightarrow 8|(n-1)(n+1)(n^2+1)$$

Euclidean Algorithm

Assume $a, b > 0$, $r_0 = a$, $r_1 = b$

- $r_0 = r_1 q_0 + r_2, 0 < r_2 < r_1$
- $r_1 = r_2 q_1 + r_3, 0 < r_3 < r_2$
- $r_2 = r_3 q_2 + r_4, 0 < r_4 < r_3$
- ...
- $r_n = r_{n+1} q_n + r_{n+2}, 0 < r_{n+2} < r_{n+1}$
- $r_{n+1} = r_{n+2} q_{n+1}$

Then $(a, b) = (r_0, r_1) = (r_1, r_2) = \dots = (r_n, r_{n+1}) = (r_{n+1}, r_{n+2}) = r_{n+2}$

Representation of Integers

Let $b > 1$. Any positive integer n can be written in form of $n = a_k b^k + \dots + a_1 b + a_0 = (a_k \dots a_1 a_0)_b$ where $0 \leq a_i < b$, a_i is called a digit in base b

Examples:

$$859 = 8 \times 10^2 + 5 \times 10 + 9$$

$$(10110)_2 = 1 \times 2^4 + 1 \times 2^2 + 1 \times 2 = (22)_{10}$$

$$(3A0F)_{16} = 3 \times 16^3 + 10 \times 16^2 + 15 \times 16 = (14863)_{10}$$

How to compute digits of n base b :

- simply apply division algorithm
- $n = bq_0 + a_0, q_0 = bq_1 + a_1, \dots$

Prime Numbers

Definition:

Any number greater than 1 whose factors are only 1 and itself is called a prime number. Otherwise; it is called composite.

Properties:

1. $p|ab \rightarrow p|a \vee p|b$
2. $(a, p) = 1 \vee p$
3. Any number has a prime factor
4. Any composite n has a prime factor p s.t. $p \leq \sqrt{n}$
5. #primes is infinity
6. #primes in form of $ak+b$ where $(a,b)=1$ is infinity
7. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 1$
8. At least a prime number exists between n and $2n$

Some Proofs

Proof (3)

using strong induction

If n is prime, we are done. Otherwise $n = ab$ where $a, b > 1$. Now consider the prime factor of a which is a factor of n

Proof (4)

$n = ab$ where $a, b > 1$. then $\min(a, b) \leq \sqrt{n}$. Now consider a prime factor of $\min(a, b)$

Proof (5)

Assume all prime numbers are $\{p_1, \dots, p_k\}$

Consider $N = p_1 \dots p_k + 1$ which has a prime factor p .
 $p|N \rightarrow (p, p_i) = 1 \rightarrow p$ is a new prime number.

Some Problems

Problem: find n s.t. $n \nmid (n-1)!$

Solution:

- If n is in form of $n = ab, a, b > 1, a \neq b$, then $n \mid (n-1)!$. Otherwise $n = p$ or p^2 where p is prime
- $n = p$ is of course is answer. If $n = p^2$, number $p, 2p$ exist in $(n-1)!$ for $p > 2$. Just check $n = 2^2$.

Problem: find n s.t. $n^2 \nmid (n-1)!$

Some Problems

Theorem:

The power of p in $n! = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$

Problem: show $\frac{(n+m)!}{n!m!}$ is integer

Solution:

We have to show for any p , the power of p in $(n+m)!$ is at least the power of p in $n!m!$

It is sufficient to show $\left\lfloor \frac{n+m}{p^i} \right\rfloor \geq \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor$ for any i

Problem: show $k!^{k^2+k+1} \mid k^3!$

Solution: show $(k^2 + k + 1) \left\lfloor \frac{k}{p^i} \right\rfloor \leq \left\lfloor \frac{k^3}{p^i} \right\rfloor$ for any prime p

Some Problems

Problem:

At least a prime number exists between n and $n!$

Solution:

One way is to show $n! \geq 2n$. The other way is to look at $n! - 1$ which is relatively prime to any number equal or less than n . So, this has a prime factor which is greater than n and of course less than $n!$.

Problem:

if p and $p^2 + 2$ are prime, then $p^3 + 2$ is prime

Solution:

$p = 3$ is the answer. Other prime numbers are of form $3k + 1$ or $3k + 2$. For both $3 \mid p^2 + 2$

Congruence

Definition:

$$a \equiv b \pmod{m} \leftrightarrow m \mid a - b$$

Properties:

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \rightarrow a \equiv c \pmod{m}$
3. $a \equiv b \pmod{m} \leftrightarrow a + c \equiv b + c \pmod{m}$
4. $a \equiv b \pmod{m} \rightarrow ac \equiv bc \pmod{m}$
5. $ac \equiv bc \pmod{m} \rightarrow a \equiv b \pmod{(m/(m, c))}$
6. $a \equiv b \pmod{m} \rightarrow a^n \equiv b^n \pmod{m}$
7. $a \equiv b \pmod{m} \rightarrow P(a) \equiv P(b)$ where P is a polynomial
8. $a \equiv r \pmod{m}$ where $a = mq + r, 0 \leq r < m$
9. $0 \leq i \neq j < m \rightarrow [i] \cap [j] = \emptyset$ where $[i] = \{x \mid x \equiv i \pmod{m}\}$

Some Proofs

Proof (5)

$$\begin{aligned}(c, m) = d &\rightarrow c = c'd, m = m'd, (c', m') = 1 \\ ac \equiv bc \pmod{m} &\rightarrow m \mid c(a - b) \rightarrow m'd \mid c'd(a - b) \\ &\rightarrow m' \mid c'(a - b), (m', c') = 1 \rightarrow m' \mid a - b \rightarrow a \equiv b \pmod{m'}\end{aligned}$$

Proof (7)

$$\begin{aligned}\text{Let } P(x) &= p_k x^k + \dots + p_1 x + p_0 \\ a \equiv b \pmod{m} &\rightarrow \forall i: p_i a^i \equiv p_i b^i \pmod{m} \rightarrow P(a) \equiv \\ &P(b) \pmod{m}\end{aligned}$$

Proof (9)

$$\begin{aligned}x \in [i] \cap [j] &\rightarrow x \equiv i \equiv j \pmod{m} \rightarrow m \mid i - j, 0 \leq i, j < m \\ &\rightarrow i = j\end{aligned}$$

Some Problems

Problem: $x \equiv 1 \pmod{2} \rightarrow x^2 \equiv 1 \pmod{8}$

Solution: $x \equiv 1 \pmod{2} \rightarrow x = 4k + 1 \vee 4k + 3 \rightarrow x^2 \equiv 1 \pmod{8}$

Problem: *Compute the remainder of 3×2^{1399} to 7*

Solution:

$$\begin{aligned} 2^3 &\equiv 1 \pmod{7} \rightarrow 2^{3 \times 466} \equiv 1 \pmod{7} \rightarrow 2^{1399} \equiv \\ &2 \pmod{7} \rightarrow 3 \times 2^{1399} \equiv 6 \pmod{7} \text{ or simply write} \\ 3 \times 2^{1399} &\equiv 3 \times 2 \times 2^{3 \times 466} \equiv 6 \times 1^{466} \equiv 6 \pmod{7} \end{aligned}$$

Problem:

Compute the rightmost digit of 1398^{1399} base 10

Solution:

$$\begin{aligned} 1398^{1399} &\equiv 8^{1399} \equiv (-2)^{1399} \equiv -2^{1399} \pmod{10} \\ 2^{1398} &\equiv 2^{4 \times 349 + 2} \equiv 1^{349} \times 2^2 \equiv 4 \pmod{5} \rightarrow 2^{1399} \\ &\equiv 8 \pmod{10} \rightarrow 1398^{1399} \equiv 2 \pmod{10} \end{aligned}$$

Some Problems

Problem: $n = (a_k \dots a_0)_{10} \rightarrow n \equiv a_k + \dots + a_0 \pmod{9}$

Solution: $n = a_k 10^k + \dots + a_1 10 + a_0, 10 \equiv 1 \pmod{9}$

Problem: Find all prime p and q s.t. $p^2 + 2q^2 = x^2$

Solution:

$p = 2 \rightarrow x = 2k \rightarrow q = 2$ but $(2,2)$ is not the answer

Otherwise, $p = 2k + 1 \rightarrow x = 2k' + 1 \rightarrow p^2 \equiv x^2 \equiv 1 \pmod{8}, p^2 + 2q^2 \equiv x^2 \pmod{8} \rightarrow 2q^2 \equiv 0 \pmod{8} \rightarrow$

$q = 2 \rightarrow (x - p)(x + p) = 8 \rightarrow$

$(x - p = 1 \wedge x + p = 8) \vee (x - p = 2 \wedge x + p = 4) \rightarrow$

$x = 3, p = 1$

but 1 is not prime

Euler's Totient Function

Definition:

$$\Phi(n) = \{x | (x, n) = 1, 1 \leq x \leq n\}, \varphi(n) = |\Phi(n)|$$
$$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(p) = p - 1$$

Theorem: $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \rightarrow \varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$

Proof: show that $(m, n) = 1 \rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

Lemma: $(a, n) = 1, i \neq j \in \Phi(n) \rightarrow ai \not\equiv aj \pmod{n}$

Lemma: $(a, n) = 1, i \in \Phi(n) \rightarrow \exists j: ai \equiv j \pmod{n}$

Then, there is a one-to-one correspondence between $\Phi(n)$ and $\{ax | x \in \Phi(n)\} \pmod{n}$. Therefore,

$$\prod_{i \in \Phi(n)} i \equiv \prod_{i \in \Phi(n)} ai \pmod{n} \text{ and } (\prod_{i \in \Phi(n)} i, n) = 1 \rightarrow$$

Theorem: $(a, n) = 1 \rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Some Problems

Problem: if d is the smallest natural number s.t. $a^d \equiv 1 \pmod{n}$ and $a^m \equiv 1 \pmod{n}$, then $d|m$

Solution:

$$m = dq + r, 0 \leq r < d, a^m \equiv a^d \equiv 1 \pmod{n} \rightarrow a^r \equiv 1 \pmod{n} \rightarrow r = 0 \rightarrow d|m$$

Problem: $n|\varphi(2^n - 1)$

Solution:

n is the smallest number s.t. $2^n \equiv 1 \pmod{2^n - 1}$

Since $2^{\varphi(2^n - 1)} \equiv 1 \pmod{2^n - 1}$, then $n|\varphi(2^n - 1)$

Wilson's Theorem

Definition:

a^* is called inverse of $a \bmod n$ iff $aa^* \equiv 1 \pmod{n}$

Lemma: (a^* exists iff $(a, n) = 1$) and $a^* \equiv a^{\varphi(n)-1} \pmod{n}$

Theorem: if p is prime, then $(p-1)! \equiv -1 \pmod{p}$

Proof:

- For any $a \in \{1, \dots, p-1\}$, inverse exists.
- If $a^* = a \rightarrow a^2 \equiv 1 \pmod{p} \rightarrow p \mid (a-1)(a+1) \rightarrow a = 1 \vee a = p-1$
- For other a , we have $a^* \neq a$
- Set $\{2, 3, \dots, p-2\}$ can be decomposed into disjoint pairs (a, b) ($a \neq b$) s.t. $ab \equiv 1 \pmod{p}$

Chinese Remainder Theorem

Theorem:

$\forall a, b \forall m, n \text{ s.t. } (m, n) = 1 \text{ we have}$

$$\exists x (x \equiv a \pmod{n} \wedge x \equiv b \pmod{m})$$

There is an unique x in $[0..mn - 1]$ satisfying above

Solution: $x \equiv bn^*n + am^*m \pmod{mn}$ where
 $nn^* \equiv 1 \pmod{m}$ and $mm^* \equiv 1 \pmod{n}$

Theorem can be extended to k linear equations:

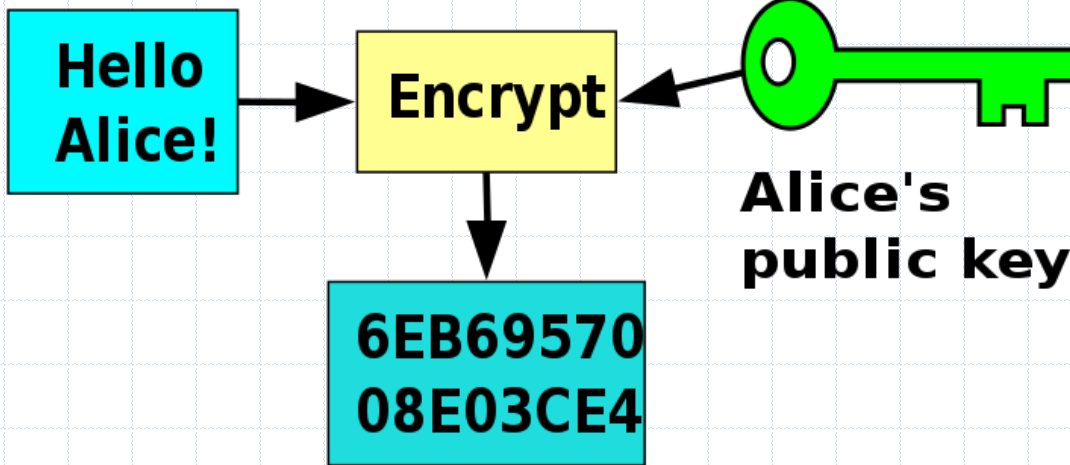
$$x \equiv a_1 \pmod{n_1} \dots x \equiv a_k \pmod{n_k} \text{ where } (n_i, n_j) = 1$$

Example:

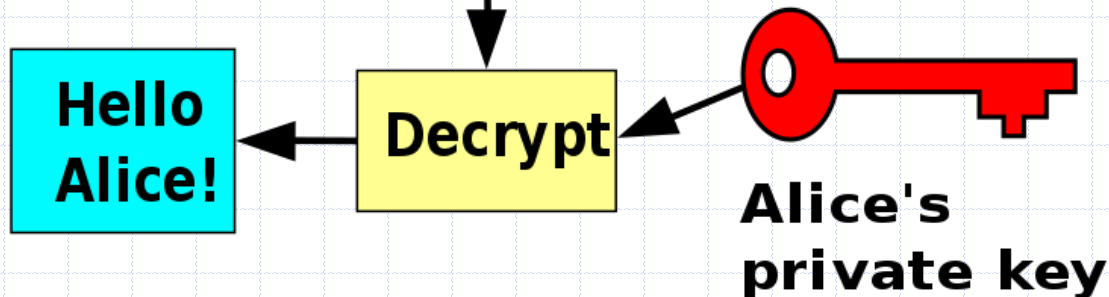
$$x \equiv 3 \pmod{7} \wedge x \equiv 5 \pmod{9} \rightarrow x \equiv 59 \pmod{63}$$

Public Key Encryption

Bob



Alice



Public Key Encryption

Let $n = pq$ where p and q are large prime numbers

Alice's key is the pair n and e where e is the number s.t. $(e, (p-1)(q-1)) = 1$. Anybody else may have this key (indeed it is a public key).

Bob's key is the pair p and q and a number d s.t. $de \equiv 1 \pmod{(p-1)(q-1)}$ (the key is private)

See message M as an integer number

Alice sends $C = M^e \bmod n$ instead of sending M

Bob computes $C^d \equiv M^{de} \equiv M^{k(p-1)(q-1)+1} \equiv M \pmod{n}$

To uniquely decrypt M , we need $M < n$. Then decompose original message into smaller pieces; each smaller than n

Without knowing p and q is hard to decrypt $M^e \bmod n$

It is hard (time-consuming) to decompose n to pq .

Miscellaneous Problems

Problem:

$$x^2 + y^2 = z^2 \leftrightarrow \exists m, n, d: x = (m^2 - n^2)d, y = 2mnd, \\ z = (m^2 + n^2)d$$

Solution:

We can assume $(x, y) = (x, z) = (y, z) = 1$, x and z are odd and y is even.

$$y^2 = (z - x)(z + x), (z - x, z + x) = 2 \rightarrow z - x = 2m^2, z + x = 2n^2 \rightarrow z = m^2 + n^2, x = m^2 - n^2, y = 2mn$$

We use the fact that $ab = x^2, (a, b) = 1 \rightarrow a = m^2, b = n^2$

The reverse is obvious. Just replace.

Miscellaneous Problems

Problem: $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$

Solution:

Let $(2^m - 1, 2^n - 1) = d$

$2^{(m,n)} - 1 \mid 2^m - 1, 2^{(m,n)} - 1 \mid 2^n - 1 \rightarrow 2^{(m,n)} - 1 \mid d$

Let r be the smallest number s.t. $2^r \equiv 1 \pmod{d}$

We know $2^n \equiv 1 \pmod{d}, 2^m \equiv 1 \pmod{d}$.

So $r \mid n, r \mid m \rightarrow r \mid (m, n) \rightarrow 2^{(m,n)} \equiv 1 \pmod{d} \rightarrow d \mid 2^{(m,n)} - 1$

Therefore, $d = 2^{(m,n)} - 1$

Miscellaneous Problems

Problem:

$$f_n = f_{n-1} + f_{n-2}, f_2 = f_1 = 1 \rightarrow (f_m, f_n) = f_{(m,n)}$$

Solution:

f_n can be extended for negative n .

$$f_0 = 0, f_{-1} = 1, f_{-2} = -1, \dots$$

We can show $f_{-2n} = -f_{2n}$ and $f_{-2n+1} = f_{2n-1}$

We can also show $\forall n, m \in \mathbb{Z}: f_{n+m} = f_{n+1}f_m + f_nf_{m-1}$

Using this and induction, we can show $k|n \rightarrow f_k|f_n$ (assume $n = ki$ and run induction on i)

Let $(f_m, f_n) = d$

$$(m, n)|n, (m, n)|m \rightarrow f_{(m,n)}|f_m, f_{(m,n)}|f_n \rightarrow f_{(m,n)}|d$$

$$\exists x, y: mx + ny = (m, n) \rightarrow f_{(m,n)} = f_{mx+ny}$$

$$= f_{mx+1}f_{ny} + f_{mx}f_{ny-1}, d|f_n|f_{ny}, d|f_m|f_{mx} \rightarrow d|f_{(m,n)}$$