Midterm 1 Friday July 8th Gradescope (2 hrs within 24 hrs) take home

5-6 problems

2 + 3 ↑ wk2 Induction sets

↑ wk1

Introduction to Number Theory

Number theory is a study of integers $\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$

Many problems are about prime numbers.

Def: We say that $a \mid b$ "a divides b" for $a, b \in \mathbb{Z}$ if $\exists\, c \in \mathbb{Z}$ s.t. $b = a \cdot c$ (or b is divisible by a)

Ex: $6 \mid 18$ $\quad 18 = 6 \cdot 3$

$10 \mid 10$ $\quad 10 = 10 \cdot 1$

$7 \mid 0$ $\quad 0 = 7 \cdot 0$ ← every integer divides zero

$3 \nmid 5$ $\quad a \nmid b$ if $\nexists\, c \in \mathbb{Z}$ s.t. $b = a \cdot c$

Properties of divisibility:

- if $a \mid b$ and $b \mid c \Rightarrow a \mid c$

Proof: $\exists d : b = a \cdot d$ $\quad \exists e : c = b \cdot e = a(d \cdot e)$ $\in \mathbb{Z}$

- $a \mid b \Rightarrow a^{1000} \mid b^{1000}$ $\quad (a^n \mid b^n)$ $n \in \mathbb{Z}$

Proof: $\exists c \in \mathbb{Z}$ s.t. $b = a \cdot c$

$b^n = (a \cdot c)^n = (a^n)(c^n)$ $\in \mathbb{Z}$

- if $a \mid x$, $a \mid y \Rightarrow a \mid mx + ny$ $\forall\, m, n \in \mathbb{Z}$

Proof: $\exists\, c, d \in \mathbb{Z}$ s.t.

$x = a \cdot c$, $y = a \cdot d$

$mx + ny = m \cdot a \cdot c + n \cdot a \cdot d = a(mc + nd)$ $\in \mathbb{Z}$

$\Rightarrow a \mid mx + ny$

Ex: $6 \mid 36^{x}$, $6 \mid 12^{y}$ $\Rightarrow$ $6 \mid 96$

$96 = \underbrace{1}_{n} \cdot 36 + \underbrace{5}_{m} \cdot 12$

Def: An even number x is s.t. $2 \mid x$

An odd number x is s.t. $2 \nmid x$

Theorem (Euclid's division algorithm)

If $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ s.t.

$$a = b \cdot q + r$$

(q: quotient, r: remainder)

Ex: $a = 100$, $b = 3$

$$100 = 3 \cdot 33 + 1$$

(q, r)

Idea: try different values of q until $100 - 3 \cdot q$ becomes negative $\Rightarrow$ too far

Proof: First find q, r, then prove uniqueness

Let $S = \{ a + b \cdot y \mid y \in \mathbb{Z} \}$

$S^+ \subset S$ - all non-negative elements of S

r - smallest element in S^+

$a = 100$, $b = 3$

$S = \{ \ldots, -5, -2, 1, 4, 7, 10, \ldots, 94, 97, 100, 103, 106, \ldots \}$

$S^+ = \{ 1, 4, 7, 10, \ldots \}$

Claim: $0 \le r < b$ since $r \in S \Rightarrow r = a + b \cdot y$ for some $y \in \mathbb{Z}$

$r \ge 0$ since $r \in S^+$

Suppose $r \ge b \Rightarrow r' = r - b = a + b \cdot y - b = a + b(y-1) \ge 0$

$\Rightarrow r' \in S^+$

Contradiction because r is the smallest element in S^+

$\Rightarrow r < b$

$r = a + b \cdot y \Rightarrow a = r + b(-y)$, with $-y = q$

Now prove uniqueness: Assume not unique $\exists\ r', q' \in \mathbb{Z}$ s.t.

$$a = b \cdot q + r \qquad 0 \le r < b$$

$$- \quad a = b q' + r' \qquad 0 \le r' < b$$

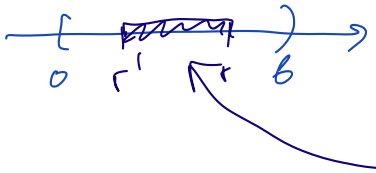
$$0 = a - a = b(q - q') + (r - r')$$

$$b(q - q') = r' - r \neq 0 \Rightarrow b \mid r' - r$$

$$|r' - r| < b$$

$\Rightarrow r' = r$

$\Rightarrow q = q'$



Ex: Show that $5 \mid n^5 - n$ $\forall n \in \mathbb{Z}_+$

1) $n=1$ $\quad n^5 - n = 0$ $\quad 5 \mid 0$

$n=2$ $\quad n^5 - n = 30$ $\quad 5 \mid 30$ ← base of induction

2) Inductive assumption: for some n $\quad 5 \mid n^5 - n$

3) Inductive step: $(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1$

$= n^5 - n + 5(n^4 + 2n^3 + 2n^2 + n)$

$n^5 - n = 5 \cdot c$; divisible by 5 ; $5 \mid n^5 - n$

$(n^4 + 2n^3 + 2n^2 + n) \in \mathbb{Z}$ $\quad = 5 \cdot d$

5 divides this number

$= 5 \mid (n+1)^5 - (n+1)$ $\quad 5(c+d)$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

Prime numbers

Def: A number $p \in \mathbb{Z}$ is prime if $p > 0$ and has exactly two divisors: 1 and p.

2, 3, 5, 7, 11, 13, 17, 19, ...

The largest known prime: $2^{74,207,281} - 1 \sim 10^{20,000,000}$

$\log_b a = \frac{\log a}{\log b}$

$\log_{10} 2 = \frac{\log 2}{\log 10} \approx 0.301\ldots$

$2^{10} = 10^{10 \cdot \log 2} \sim 10^3$ (3)

$2^{100} \sim 10^{30}$

$\pi(x) = \#$ primes $< x$

$\pi(10) = 4$

$\pi(20) = 8$ ←

$\pi(x) \asymp \frac{x}{\log x}$

$x = 20$ $\quad \frac{20}{\log 20} \approx 6.7$

Theorem: There are infinitely many primes

idea: $a \mid b$, $a > 1$

$a \nmid b+1$

$6 \mid 12$ $\quad 7 \mid 21$

$6 \nmid 13$ $\quad 7 \nmid 22$

$\exists c \in \mathbb{Z}$ s.t. $b = a \cdot c$

assume $a \nmid b+1 \Rightarrow \exists d \in \mathbb{Z}$ s.t. $b+1 = a \cdot d$

$a \cdot c + 1 = a \cdot d$

$1 = a(d-c) \Rightarrow a \mid 1$

$\Rightarrow a = 1$

$100 = 5 \cdot 20$ (b, c, a)

$101 \Rightarrow 6 \cdot 20$

$120 = 6 \cdot 20$

	20	40	60	80	100	120
c	1	2	3	4	5	6

Proof: Assume there are finitely many primes

$\{p_1, p_2, \dots p_k\}$ – complete list of all primes.

$N = p_1 \cdot p_2 \cdot \dots \cdot p_k$ by construction $p_i \mid N$, $i = 1, \dots, k$

but $p_i \nmid N+1$, $i = 1, \dots, k$

Does $N+1$ have any divisors?

Yes: • $1, N+1$ and no other divisors $\Rightarrow N+1$ is prime

• $N+1 = a \cdot b$, $a, b < N+1$

$a \mid N+1$

How about a?

If a has a and 1 as its only divisors $\Rightarrow a$ prime

O/w $a = c \cdot d$, $c, d < a$

How about c?

⋮

the process terminates when we find a prime p s.t. $p \mid N+1$

$p \neq p_1, p_2, \dots p_k$

$\Rightarrow$ contradiction so set of primes is infinite.

Finding primes

Sieve of Eratosthenes

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

do over (2 → smallest non-crossed num)

– cross out all multiples of 2 except 2

– circle the first non crossed number

$\pi(36) = 10$

Ex: run the loop 3 times

Q: Given $N \in \mathbb{N}$ how many times do you need to run the algorithm?

A: $\sqrt{N}$ — If $a > \sqrt{N}$, pick $K < N$ (so $K \sim N$)

$a \mid K \Rightarrow K = a \cdot c$ $\quad (c \mid 4)$

$c < \sqrt{N}$

Find the largest a s.t. $a^2 \leq N$

Pick $K < N$: $K = a \cdot c$ $\quad c < \sqrt{N}$

c has already been crossed out

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31

1 2 2 4 2 4 2 4 6 2

congruent to

$4k+1$: 5, 13, 17, 29 ... $\equiv 1 \pmod 4$

$13 \equiv 1 \pmod 4$

$4k+3$: 3, 7, 19, 23 ... $\equiv 3 \pmod 4$

Proposition: Given any N there are two consecutive primes which are $\geq N$ apart from each other.

... p_k ... ... p_{k+1}, ... — no primes between, $\geq N$

$\Longleftrightarrow \quad p_{k+1} - p_k \geq N$

$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt$

Stirling approximation: $n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdots$

$e^{(n-\frac{1}{2})\log n}$

$\sim e^{24}$

$\sim 10^9$

Proof: $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n-1) \cdot n$

$$\begin{cases} a_1 = (n+1)! + 2 \\ a_2 = (n+1)! + 3 \\ \vdots \\ a_i = (n+1)! + i + 1 \\ \vdots \\ a_n = (n+1)! + n + 1 \end{cases}$$

$n = 10$

$a_1 = 11! + 2 = 481,466,702$

$a_2 = 11! + 3 = 481,466,703$

$\vdots$

$(i+1) \mid a_i$ since $(n+1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (i+1) \cdot \ldots \cdot n \cdot (n+1)$

$\left(\frac{(n+1)!}{\quad}\right)$

$a_i = (i+1)\left(\frac{(n+1)!}{i+1} + 1\right)$, so all a_i are composite

$\uparrow$ $\mathbb{Z}$ $\qquad n = N-1$

The Fundamental Theorem of Arithmetic (FTA)

For any integer $N > 1$ there is a prime factorization of N:

There are distinct primes $p_1, p_2 \dots p_k$, and $r_1, \dots, r_k$, $r_i \geq 1$, $r_i \in \mathbb{Z}$ (multiplicities)

s.t. $N = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \dots \cdot p_k^{r_k}$

This factorization is unique up to reordering.

$16 = 2^4$ $\qquad p_1 = 2, \ r_1 = 4$

$40 = 2^3 \cdot 5$ $\qquad p_1 = 2, \ r_1 = 3$, $p_2 = 5, \ r_2 = 1$

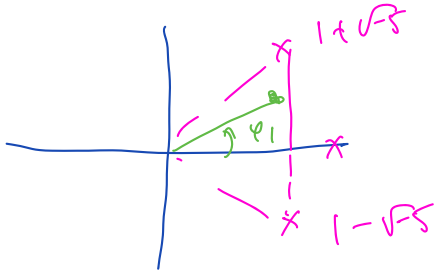
Ex: $\mathbb{Z}$ - ring $\qquad \mathbb{C} = \mathbb{R}[\sqrt{-1}] \qquad i^2 = -1$, $x^2 + 5 = 0$

Gaussian numbers (ring) $\rightarrow$ $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\} \supset \mathbb{Z}$

$\mathbb{Z}$ adjoin element $\sqrt{-5}$

- $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$
- $2 \cdot 3 = 6$

$\Rightarrow$ Gaussian prime decomposition is not unique!



$z_1 = |z_1| \cdot e^{i\varphi_1}$

$z_1 \cdot z_2 = |z_1|(z_2| \cdot e^{i\varphi_1 + i\varphi_2}$

Def: Let $a, b \in \mathbb{Z}$ not both equal to zero. The greatest common divisor of a and b $\qquad \gcd(a,b) = (a,b) = d$

is the largest integer that divides a and b.

Ex: $\gcd(6, 15) = 3$ ($2 \cdot 3$, $3 \cdot 5$)

$\gcd(105, 0) = 105$

$\gcd(100, 76) = 2^2 = 4$ ($2^2 \cdot 5^2$, $2^2 \cdot 19$)

$\gcd(2022, 2022^{2022}, 2022^{2022}) - ?$

Division algorithm

Idea: $a, b \in \mathbb{Z}$ $\quad a = b \cdot q + r$, $0 \le r < b$

$\gcd(a,b)$ $\quad \gcd(b,r)$

Ex:

$\gcd(126, 27) = 3^2 = 9$

$126 = 27 \cdot 4 + 18$

$\gcd(27, 18) = 9$

Ex: $a = 502$, $b = 98$

$502 = 98 \cdot 5 + 12$

$\gcd(502, 98) = 2$

$\gcd(98, 12) = 2$

A B

Lemma: Let $a, b \in \mathbb{Z}$, $a, b \neq 0$. Then $\gcd(a,b) = \gcd(b,r)$ where $r = a - b \cdot q$ for some $q \in \mathbb{Z}$, $0 \le r < b$.

Proof: $\{A = B\} \Leftrightarrow \{A \ge B\} \wedge \{B \ge A\}$.

Let $c \in \mathbb{Z}$, $c \mid a$, $c \mid b$ $\Rightarrow$ $c \mid (a \cdot 1 + b \cdot (-q))$, $q \in \mathbb{Z}$ (quotient)

($\ge$) $\Rightarrow c \mid r$

$\Rightarrow \gcd(a,b) \mid r$

So $\gcd(b,r) \ge \gcd(a,b)$

($\le$) Let $d \mid b$, $d \mid r$ $\Rightarrow$ $d \mid (b \cdot q + r) = d \mid a$ (a), $d \in \mathbb{Z}$

$\Rightarrow \gcd(b,r) \mid a$

So $\gcd(a,b) \ge \gcd(b,r)$

Therefore $\gcd(b,r) = \gcd(a,b)$.

Algorithm of computing of $\gcd(a,b)$ (Euclid)

- $a = b \cdot q_1 + r_1$ $\quad 0 \le r_1 < b$ $\quad \gcd(a,b) = \gcd(b,r_1)$ (Lemma)
- $b = r_1 \cdot q_2 + r_2$ $\quad 0 \le r_2 < r_1$ $\quad \gcd(b,r_1) = \gcd(r_1,r_2)$
- $r_1 = r_2 \cdot q_3 + r_3$ $\quad 0 \le r_3 < r_2$ $\quad \gcd(r_1,r_2) = \gcd(r_2,r_3)$

⋮

⋮

- $r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1}$ $\quad 0 \le r_{k-1} < r_{k-2}$ $\quad \gcd(r_{k-3}, r_{k-2}) = \gcd(r_{k-2}, r_{k-1})$
- $r_{k-2} = r_{k-1} \cdot q_k + r_k$, $r_k = 0$ $\quad \gcd(r_{k-2}, r_{k-1}) = \gcd(r_{k-1}, 0) = r_{k-1}$

$r_{k-1} = \gcd(a, b)$

Ex: $\gcd(12, 10) = 2$ ($a = 12$, $b = 10$, $q_1 = 1$, $r_1 = 2$)

$12 = 10 \cdot 1 + 2$

$10 = 2 \cdot 5 + 0$ (q_1, r_1, q_2, r_2)

Ex: $\gcd(60, 37) = 1$

$60 = 37 \cdot 1 + 23$

$37 = 23 \cdot 1 + 14$

$23 = 14 \cdot 1 + 9$

$14 = 9 \cdot 1 + 5$

$9 = 5 \cdot 1 + 4$

$5 = 4 \cdot 1 + 1$

$4 = 4 \cdot 1 + 0$

Ex: $\gcd(2022\,2022\,2022,\ 20222022) = 2022$

$2022\,2022\,2022 = 20222022 \cdot 10000 + 2022$

$20222022 = 2022 \cdot 10000 + 2022$

$= 2022 \cdot 10001 + 0$

Ex: $a = b \cdot q + r$ $\quad a \ge b$

$\gcd(27, 15) = 3$

1) $27 = 15 \cdot 1 + 12$

$15 = 12 \cdot 1 + 3$

$12 = 3 \cdot 4 + 0$

2) $15 = 27 \cdot 0 + 15$

$27 = 15 \cdot 1 + 12$

$15 = 12 \cdot 1 + 3$

$12 = 3 \cdot 4 + 0$

Theorem: Let $a, b \in \mathbb{Z}$, not both equal to zero.

Then $\gcd(a, b) = \min \{ Xa + Yb \mid X, Y \in \mathbb{Z},\ Xa + Yb > 0 \}$

(min: smallest number in set)

Ex: $\gcd(701, 33) = 701 \cdot X + 33 \cdot Y = 1$

Euclid: $701 = 33 \cdot 21 + 8$

$33 = 8 \cdot 4 + 1$

$8 = 1 \cdot 8 + 0$

$1 = 33 - 8 \cdot 4 = 33 - (701 - 33 \cdot 21) \cdot 4$

$= 33 - 701 \cdot 4 + 33 \cdot 84$

$= 701 \cdot \underbrace{(-4)}_{X} + 33 \cdot \underbrace{85}_{Y}$

Ex:

$\gcd(60, 37)$

6 $60 = 37 \cdot 1 + 23$

5 $37 = 23 \cdot 1 + 14$

4 $23 = 14 \cdot 1 + 9$

3 $14 = 9 \cdot 1 + 5$

2 $9 = 5 \cdot 1 + 4$

1 $5 = 4 \cdot 1 + \boxed{1}$

$1 = 5 - 4 = 5 - (9 - 5)$

$= 5 \cdot 2 - 9$

$\overset{3}{=} (14 - 9) \cdot 2 - 9 = 14 \cdot 2 - 9 \cdot 3$

$\overset{4}{=} 14 \cdot 2 - (23 - 14) \cdot 3 = 14 \cdot 5 - 23 \cdot 3$

$\overset{5}{=} (37 - 23) \cdot 5 - 23 \cdot 3 = 37 \cdot 5 - 23 \cdot 8$

$\overset{6}{=} 37 \cdot 5 - (60 - 37) \cdot 8$

$= 37 \cdot \underbrace{13}_{Y} + 60 \cdot \underbrace{(-8)}_{X}$

Theorem: Let $a, b \in \mathbb{Z}$, not both equal to zero.

Then $\gcd(a, b) = \min \{ Xa + Yb \mid X, Y \in \mathbb{Z},\ Xa + Yb > 0 \}$

(min: smallest number in set)

Proof: $S = \{ Xa + Yb \mid X, Y \in \mathbb{Z} \}$

$S^+ = \{ \text{positive elements of } S \}$

1) Show that the minimum divides a and b

Let $ma + nb$ be the smallest element of S^+

Division algorithm $a = (ma + nb) \cdot q + r, \quad 0 \le r < ma + nb$

$r = a - (ma + nb) q = a \underbrace{(1 - mq)}_{X} + b \underbrace{(-nq)}_{Y}$

if $r \neq 0$ then $r = aX + bY \in S^+$

but $r < ma + nb$, contradiction

since $ma + nb$ is the smallest element in S^+

which means $r = 0$.

so $ma + nb \mid a$

Analogously, $ma + nb \mid b$ (Exercise)

2) Show that $ma+nb = \gcd(a,b)$

Since $\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$ $\Rightarrow$ $\gcd(a,b) \mid ma+nb$

$\hookrightarrow$ $\gcd(a,b) \le ma+nb$

According to step 1) $ma+nb \mid a$, $ma+nb \mid b$ $\Rightarrow$ $ma+nb \le \gcd(a,b)$

$\Downarrow$

$\gcd(a,b) = ma+nb$.

Def: Let $a, b \in \mathbb{Z}$. We say that a and b are relatively prime (coprime) (mutually) if $\gcd(a,b)=1$.

Ex: $\gcd(17, 24) = 1$

$\gcd(2^k, 3^n) = 1 \quad \forall k, n$

Lemma: Let $a, b, c \in \mathbb{Z}$, $\gcd(a,b)=1$ and $a \mid b \cdot c$.

Then $a \mid c$

Proof: $\gcd(a,b)=1$ then by the theorem above $1 = aX+bY$, $X, Y \in \mathbb{Z}$

$\times c$: $c(aX+bY) = c$

$a \cdot c \cdot X + b \cdot c Y = c$

We know that $a \mid b \cdot c \Rightarrow a \mid b \cdot c \cdot Y$, $a \mid a \cdot c \cdot X$ $\Rightarrow$ $a \mid \underbrace{bcY + acX}_{c} \Rightarrow a \mid c$.

Ex: $\gcd(17, 24) = 1$ (a, b) $\quad 17 \mid 24 \cdot 17 \cdot 5$ (a, b, c)

$\gcd(14, 24) = 2$ (c, b) $\quad 17 \mid 17 \cdot 5$

Corollary: (Euclid) p is prime iff for $a, b \in \mathbb{Z}$ s.t. $p \mid a \cdot b$ we must have $p \mid a$ or $p \mid b$.

Proof: $\Rightarrow$ Suppose p is prime, $p \mid a \cdot b$ (a, b, c)

$\gcd(p, a) = p$ or 1

If $\gcd(p,a) = 1 \overset{\text{Lemma}}{\Rightarrow} p \mid b$

If $\gcd(p,a) = p \Rightarrow p \mid a$

$\Leftarrow$ Suppose $\forall a, b \in \mathbb{Z}$ s.t. $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$

Assume p is not prime $p = x \cdot y$, $x, y \neq 1$

then $p \mid x \cdot y \Rightarrow p \mid x$ or $p \mid y$

but $p = x \cdot y$ so $x, y < p$

Contradiction, so p is prime.

Corollary: If p is prime and $p \mid a_1 \cdot a_2 \cdots a_n \Rightarrow p \mid a_i$ for some i.

($a_2 \cdots a_n = b_1$)

Prove by iterations

The Fundamental Theorem of Arithmetic (FTA)

For any integer $N > 1$ there is a prime factorization of N:

There are distinct primes $p_1, p_2 \cdots p_k$, and $r_1, \ldots, r_k$, $r_i \geq 1$, $r_i \in \mathbb{Z}$ (multiplicities)

s.t.

$$N = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \cdots \cdot p_k^{r_k}$$

This factorization is unique up to reordering.

Proof: (Existence) Suppose there are integers >1 w/o prime factorization

let $n > 1$ be smallest such number

- if $n = p$ - prime then it has a factorization, contradiction
- $n = a \cdot b$, $1 < a, b < n$

Since $a, b < n \Rightarrow a, b$ have prime factorizations

$a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, $b = q_1^{s_1} \cdots q_m^{s_m}$

$n = p_1^{r_1} \cdots p_k^{r_k} \cdot q_1^{s_1} \cdots q_m^{s_m}$

If $p_i = q_j$ for some i, j

then $p_i^{r_i} \cdot q_j^{s_j} \to p_i^{r_i + s_j}$

So n has a factorization.

Ex:

$54 = 6 \cdot 9 = 2 \cdot 3^3$

$6 = 2 \cdot 3$, $9 = 3^2$

$2 \to p_1, r_1 = 1$

$3 \to q_1 = 3$, $s_1 = 2$

$3 \to r_2 \leq s_1$

(Uniqueness) Suppose $q_1^{b_1} \cdots q_s^{b_s} = n = p_1^{a_1} \cdots p_r^{a_r}$

Need to show that $s = r$

Without loss of generality assume $r \leq s$

- $p_1 \mid n \Rightarrow p_1 \mid q_1^{b_1} \cdots q_s^{b_s} \overset{\text{Coroll 2}}{\Rightarrow} p_1 \mid q_i^{b_i}$ for some i

$\Rightarrow p_1 \mid q_i \Rightarrow p_1 = q_i$

Relabel $q_1^{b_1} \cdots q_i^{b_i} \cdots q_s^{b_s} \to p_1^{b_1} \cdot q_2^{b_2} \cdots q_s^{b_s}$

- $p_2 \mid n \Rightarrow p_2 \mid p_1^{b_1} \cdot q_2^{b_2} \cdots q_s^{b_s} \overset{\text{Coroll 2}}{\Rightarrow} p_2 \mid q_2^{b_2} \cdots q_s^{b_s}$

$\Rightarrow p_2 \mid q_j^{b_j}$ for some $2 \leq j \leq s$

$\Rightarrow p_2 \mid q_j \Rightarrow p_2 = q_j$

Relabel $p_1^{b_1} q_2^{b_2} \cdots q_j^{b_j} \cdots q_s^{b_s} \longrightarrow p_1^{b_1} p_2^{b_2} q_3^{b_3} \cdots q_s^{b_s}$

$\vdots$

j

Until $p_r = q_r$

Now let us show that $s = r$. Suppose $s > r$

$$q_{r+1} \mid n = q_{r+1} \mid p_1^{a_1} \cdots p_r^{a_r}$$

Corr $\Rightarrow q_{r+1} \mid p_\ell$ for some ℓ

$\Rightarrow q_{r+1} = p_\ell$.

Contradiction

$$q_1^{b_1} \cdots q_s^{b_s} = n = p_1^{a_1} \cdots p_r^{a_r}$$

We have shown: $q_1^{a_1} \cdots q_r^{a_r} = n = q_1^{b_1} \cdots q_n^{b_n}$

still need to show: $a_i = b_i$ $\forall i$ (Exercise).

Ex: $3^2 \cdot 7^4$ vs $3^5 \cdot 7^1$

Theorem: Let $a, b \in \mathbb{Z}$, $a, b > 1$

by FTA: $a = p_1^{r_1} \cdots p_n^{r_n}$ $r_i \geq 0$ $\forall i$

$b = p_1^{s_1} \cdots p_n^{s_n}$ $s_i \geq 0$

Then $\gcd(a, b) = p_1^{\min(r_1, s_1)} \cdot p_2^{\min(r_2, s_2)} \cdots p_n^{\min(r_n, s_n)}$

Ex: $\gcd(7, 82) = 1$

$82 = 2 \cdot 41 = 2^1 \cdot 7^0 \cdot 41^1$

$7 = 2^0 \cdot 7^1 \cdot 41^0$

$2^{\min(0,1)} \cdot 7^{\min(1,0)} \cdot 41^{\min(1,0)} = 1$

Ex: $\gcd(124, 74)$

$124 = 2^2 \cdot 31^1 \cdot 37^0$

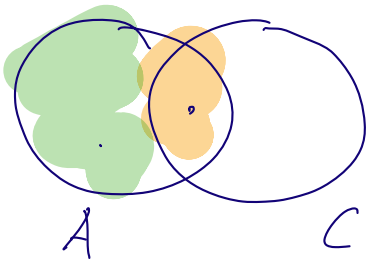
$74 = 2^1 \cdot 31^0 \cdot 37^1$

$\gcd(124, 74) = 2^1 \cdot 31^0 \cdot 37^0 = 2$

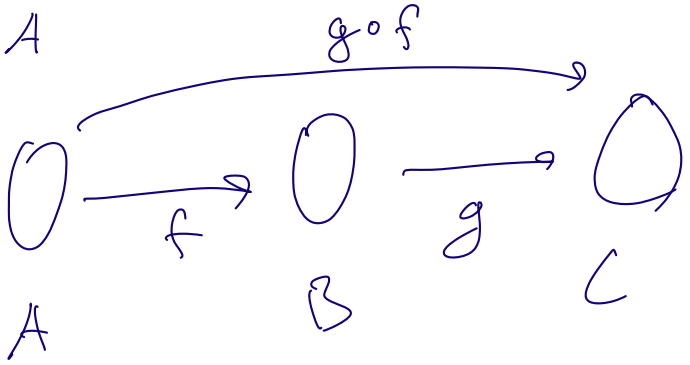
$A \subseteq B$

let $x \in A$ → $x \in C \Rightarrow x \in A \cap C \Rightarrow x \in B \cap C \Rightarrow x \in B$

→ $x \notin C \Rightarrow x \in A \cup C \Rightarrow x \in B \cup C \Rightarrow x \in B$

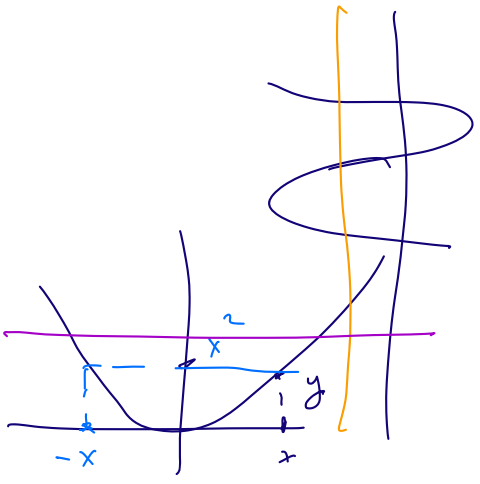


$B \subseteq A$



$\mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R}$

$x \xmapsto{f} x^2 \xmapsto{g} x^{3/2}$



$\forall x \; \exists ! \; y \text{ s.t. } y = f(x)$

$x \mapsto |x|^3$

$A = \{0, 1\}$ ↓ f

$B = \{0, 1, 2\}$ ↓ g

$C = \{0, 1\}$

$(-1) \mapsto 1 \mapsto 1$

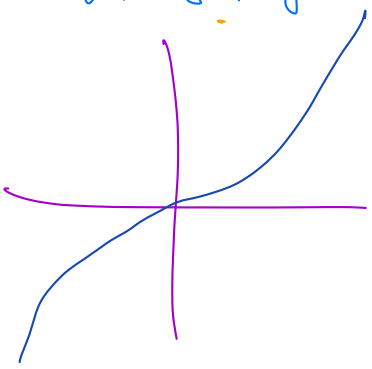
$(x^2)^{3/2} \to |x|^3$

$g(f(x)) = |x|^3$

$g \circ f = id$

$0 \mapsto 0$

$1 \mapsto 1$



$n \mid (n+1)^n - 1$

$5 \mid n^5 - n$

- base: $n = 1$ $\quad (1+1)^1 - 1 = 1$ ✓✓✓
- Assume holds for some n
- Show for $n+1$:

$(n+2)^{n+2} - 1 = (n+2)^n \cdot (n+2) - 1$

$= (n+2)^n \cdot (n+1) + (n+1)^n - 1$

$\sum_{k}^{n} \binom{n}{k} (n+1)^{n-k}$

$$\binom{n}{n}\cdot(n+1)^0 \sum_{k=0}^{n-1}\binom{n}{k}(n+1)^{n-k} \quad \cancel{+1=+}$$

Triangular numbers

T_1 T_2 T_3 T_4 T_5 T_n

1 3 6 10 15

$$T_{n+1} = T_n + n+1$$

$$T_n = \frac{n(n+1)}{2}$$

$$\frac{1}{1-x} = 1+x+x^2+x^3+\dots = \sum_{n\geq 0} x^n \qquad \{1,1,1,\dots\}$$

$$\frac{1}{(1-x)^2} = 0+1+2x+3x^2+\dots = \sum_{n=0}^{\infty} n\cdot x^{n-1} \qquad \{1,2,3,\dots\}$$

$$\frac{2}{(1-x)^3} = 0+0+2+6x+\dots = \sum_{n=0}^{\infty} n\cdot(n-1)\,x^{n-2}$$

$$\frac{1}{(1-x)^3} = 1+3x+6x^2+\dots = \sum_{n=1}^{\infty} \frac{n(n-1)}{2}\,x^{n-2} \qquad n-1 \mapsto n$$

$$\frac{x}{(1-x)^3} = x+3x^2+6x^3+10x^4+\dots = \sum_{n=1}^{\infty} \frac{n(n-1)}{2}\,x^{n-1}$$

$$= \sum_{n=1}^{\infty} \frac{n(n+1)}{2}\,x^n$$

$$T(x) = \sum_{n\geq 1}^{\infty} T_n x^n$$

$$T(x) = x + \sum_{n=2}^{\infty} T_n x^n = x + \sum_{n=2}^{\infty} (T_{n-1}+n)\,x^n$$

$$= x + \sum_{n=2}^{\infty} T_{n-1}x^n + \sum_{n=2}^{\infty} n\,x^n = x\cdot\sum_{n=2}^{\infty} n x^{n-1}$$

$$\downarrow$$

$$T_1 x^2 + T_2 x^3 + \dots$$

$$= x\,(T_1 x + T_2 x^2 + \dots) = x\cdot T(x)$$

$$T(x) = x + x\cdot T(x) + x\left(\frac{1}{(1-x)^2} - 1\right) = x\,T(x) + \frac{x}{(1-x)^2}$$

$$T(x)(1-x) = \frac{x}{(1-x)^2} \Rightarrow T(x) = \frac{x}{(1-x)^3}$$

Def: The least common multiple of a and b $\operatorname{lcm}(a,b)$ is the smallest integer d s.t. $a \mid d$, $b \mid d$

Note: $\operatorname{lcm}(a,b) \le a \cdot b$

Ex: $\operatorname{lcm}(10,35) = 70$

$\operatorname{lcm}(8,34) = 2^3 \cdot 17 = 136$ ($34 = 17 \cdot 2$)

$\operatorname{lcm}(7,6) = 42$

Theorem: Let $a, b > 1$, $a = p_1^{r_1} \cdots p_n^{r_n}$, $b = p_1^{s_1} \cdots p_n^{s_n}$, $r_i, s_i \ge 0$

then $\operatorname{lcm}(a,b) = p_1^{\max(r_1,s_1)} \cdot p_2^{\max(r_2,s_2)} \cdot \cdots \cdot p_n^{\max(r_n,s_n)}$

Ex: $a = 2^2 \cdot 3^4 \cdot 5^3 \cdot 19^{19} \cdot 71^0$

$b = 2^0 \cdot 3^2 \cdot 5^0 \cdot 19 \cdot 71^1$

$\operatorname{lcm}(a,b) = 2^2 \cdot 3^4 \cdot 5^3 \cdot 19^{19} \cdot 71^1$

Theorem: $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b \Rightarrow \operatorname{lcm}(a,b) = \dfrac{a \cdot b}{\gcd(a,b)}$

Proof: $a = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_n^{r_n}$

$b = p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n}$

$a \cdot b = p_1^{r_1+s_1} \cdots p_n^{r_n+s_n}$

$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = p_1^{\min(r_1,s_1) + \max(r_1,s_1)} \cdot \cdots \cdot p_n^{\min(r_n,s_n) + \max(r_n,s_n)}$

the two are equal since

$\min(r_i, s_i) + \max(r_i, s_i) = r_i + s_i \quad \forall i.$

We can find $\operatorname{lcm}(a,b)$ using division algorithm.

$\gcd(18,15) = 3$

$18 = 15 \cdot 1 + 3$

$15 = 3 \cdot 5 + 0$

$\operatorname{lcm}(18,15) = \dfrac{18 \cdot 15}{3} = 90$

Primes in arithmetic progressions

$a, a+b, a+2b, a+3b, \ldots$ $\quad a, b \in \mathbb{Z}_+$

5, 10, 15, 25, 30 ... $\quad a=5, b=5$

1, 8, 15, 22, 29, 36, 43 $\quad a=1, b=7$

1, 3, 5, 7, 9, 11, 13, 15 $\quad a=1, b=2$

When do we have infinitely many primes in an arithmetic progression?

Suggestions: $\gcd(a,b)=1$?

$a \mid b$? $b \mid a$?

Ex: $a=15, b=18$ $\quad \gcd(15,18)=3$

15, 33, 51, 69, 87 ... no primes

Not infinitely many primes if $\gcd(a,b) \mid a+nb$ for all n except a few.

Theorem (Dirichlet) The arithmetic progression

$a, a+b, a+2b, a+3b, \ldots$

has infinitely many primes iff $\gcd(a,b)=1$

Special case: $a=3, b=4$

3, 7, 11, 15, 19, 23, 27

$\{4n+3 \mid n \geq 0\}$

Theorem: There are infinitely many primes of the form $4n+3$

Proof: Assume false, $p_0=3, p_1=7 \ldots p_{r-1}, p_r$

construct $N = 4 \cdot p_1 \cdots p_r + 3$ - new prime

Claim: p is either of the form $4n+1$

or $4n+3$

$\pi(X) \rightsquigarrow \pi(X, a, b) = \#\{\text{primes } p \leq X \mid p = a+bn, n \in \mathbb{Z}_+\}$

If $\gcd(a,b)=1 \Rightarrow \pi(X,a,b) = F(a) \cdot \frac{X}{\log X}$

In particular, $\pi(X,1,4) \sim \frac{1}{2} \frac{X}{\log X}$

$\pi(x, 3, 4)$

Chebyshev's bias.

$4n+1$	$4n+3$
5	3
13	7
29	11
37	19
41	23
53	31
61	43
73	47
	59
	67

Congruences modulo m

$a \equiv b \pmod m$ — a is congruent to b modulo m

if $m \mid a-b$ or $a = m \cdot q + b$ for some $q \in \mathbb{Z}$.

Ex: $14 \equiv 2 \pmod{12}$

$14 = 12 \cdot 1 + 2$

$5 \equiv 26 \pmod 3$

Thm: If $a \equiv b \pmod c$ and $d \equiv e \pmod c$

Then: 1) $a+d \equiv b+e \pmod c$

2) $a \cdot d \equiv b \cdot e \pmod c$

Proof: 1) $(b+e)-(a+d) = (b-a)+(e-d) \Rightarrow c \mid (b-a)+(e-d)$

$c \mid (b-a)$ $\quad c \mid (e-d)$

2) $ad - bd + bd - be = (a-b)\cdot d + (d-e)\cdot b$

$c \mid (a-b)$ $\quad c \mid (d-e)$

$\Rightarrow c \mid (a-b)\cdot d + (d-e)\cdot b \Rightarrow c \mid ad - be$

"$\equiv$" is an equivalence relation

- $a \equiv a \pmod c$ $\quad a = 0 \cdot c + a$

- $a \equiv b \pmod c \Rightarrow b \equiv a \pmod c$ $\quad a = q\cdot c + b$, $b = (-q)\cdot c + a$

- $a \equiv b \pmod c$, $b \equiv d \pmod c$

$\Rightarrow a \equiv d \pmod c$

$c \mid (b-a)$, $c \mid d-b \Rightarrow c \mid \underbrace{b-a+d-b}_{d-a}$.

Equivalence classes: mod 5

$-9, -4, 1, 6, 11, 16, 21, 26, 31$ $\quad \leftarrow \quad \equiv 1 \pmod 5$

$12, 17, 22 \ldots$ $\quad \equiv 2 \pmod 5$

residue classes

$\equiv 0 \pmod 5$

Ex: $26\cdot 5 + 19\cdot 38 + 15\cdot 422 \equiv 0 \pmod 6$

$26 \equiv 2 \pmod 6$, $5 \equiv 5 \pmod 6$

$26\cdot 5 \equiv 2\cdot 5 \equiv 4 \pmod 6$

$19 \equiv 1 \pmod 6$

$38 \equiv 2 \pmod 6$

$422 \equiv 2 \pmod 6$

$15 \equiv 3 \pmod 6$

Powers of integers modulo p

Ex: $a \in \mathbb{Z}$ $\quad a^1, a^2, a^3 \ldots \pmod p$

1) $a=2$, $p=3$

$2^1 \equiv 2 \pmod 3$

$2^2 \equiv 1$

$2^3 \equiv 2$

$2^4 \equiv 1$

$2^5 \equiv 2$

$2^6 \equiv 1$

2) $a=2$, $p=5$

$2^1 \equiv 2 \pmod 5$

$2^2 \equiv 4 \pmod 5$

$2^3 = 3$

$2^4 \equiv 1$

$2^5 \equiv 2$

$2^6 \equiv 4$

$2^7 \equiv 3$

$2^8 \equiv 1$

3) $a=3$, $p=7$

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 2$

$3^3 \equiv 6$

$3^4 \equiv 4$

$3^5 \equiv 5$

$3^6 \equiv 1$

$3^7 \equiv 3$

$3^8 \equiv 2$

$3^9 \equiv 6$

$3^{10} \equiv 4$

$3^{20} \equiv 2$

Little Fermat's theorem: If p is prime, $a \in \mathbb{Z}$ s.t. $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

Solving Linear Congruences

$2x = 4 \rightarrow x = 2$

$2x = 3 \rightarrow x = 3/2$

$0 \cdot x = 1 \rightarrow$ no solution

- $2x \equiv 3 \pmod{5}$ Solve for $x \in \mathbb{Z}$

  $x = 4, 9, 14, \ldots$

  $x = 4 + 5n, \; n \in \mathbb{Z}$

- $4x \equiv 8 \pmod{18}$

  $x = 2, 20, 38 \ldots$ $\quad 2 + 18 \cdot n$

- $2x \equiv 3 \pmod{6}$ $\quad 2x = 6n + 3$ ← impossible.

Theorem: Let $a, b, m \in \mathbb{Z}$, $m \neq 0$. Then $ax \equiv b \pmod{m}$ has a solution iff $\gcd(a, m) \mid b$

Proof: ($\Rightarrow$): Suppose $ax \equiv b \pmod{m}$ has a solution $x = k$

$ak \equiv b \pmod{m} \Rightarrow m \mid ak - b$

$\exists y \in \mathbb{Z}$ s.t. $m \cdot y = ak - b$

$\Rightarrow b = a \cdot k - my = a \cdot k + m(-y)$

$\gcd(a, m) \mid a$ $\quad \gcd(a, m) \mid m$

$\Rightarrow \gcd(a, m) \mid \underbrace{a \cdot k + m(-y)}_{b}$

($\Leftarrow$): suppose $\gcd(a, m) \mid b$

$\rightarrow \exists k \in \mathbb{Z}$ s.t. $k \cdot \gcd(a, m) = b$

$\exists C, D \in \mathbb{Z}$ s.t. $\gcd(a, m) = C \cdot a + D \cdot m$

$\Rightarrow k(C \cdot a + D \cdot m) = b$

$a \cdot k \cdot C + m \underbrace{kD}_{\mathbb{Z}} = b$

$a \cdot kc = -m \cdot k + b \Rightarrow \underbrace{a \cdot kc}_{x} \equiv b \pmod m$

$x = kc$ solves the problem.

Note: $k = \frac{b}{\gcd(a,m)}$

Ex: $15x \equiv 100 \pmod{52}$

$\gcd(15,52) = 1$

$52 = 15 \cdot 3 + 7$

$15 = 7 \cdot 2 + 1$ ← running backwards

$7 = 1 \cdot 7 + 0$

$1 = 15 - 7 \cdot 2 = 15 - (52 - 15 \cdot 3) \cdot 2$

$= 15 \cdot 7 + 52(-2)$

$c = 7$

$k = \frac{100}{1} = 100$

$x = 7 \cdot 100 = 700 \equiv 24 \pmod{52}$

$x = 24$

$x = 24 + 52 \cdot n, \quad n \in \mathbb{Z}$

Thm: Let $a, b, m \in \mathbb{Z}$, $m \neq 0$, $d = \gcd(a,m)$, $d \mid b$

then there are exactly d incongruent solutions $(\bmod m)$ to $ax \equiv b \pmod m$.

Given x_0 - a solution of the problem, then the set of all incongruent solutions:

$$\left\{ x_0, x_0 + \underbrace{\frac{m}{d}}_{t}, x_0 + \frac{m}{d} \cdot 2, \dots x_0 + \frac{m}{d}(d-1) \right\}.$$

Ex: $12x \equiv 30 \pmod{42}$

$\gcd(12,42) = 6$

$\frac{42}{6} = 7$

$x_0 = 6$ - a solution

$6 + n \cdot 42$	$6 + 7 + n \cdot 42$	$6 + 14 + n \cdot 42$	$6 + 7 \cdot 3$	$6 + 7 \cdot 4$	$6 + 7 \cdot 5$

Proof: Let x_0 be a solution of $ax \equiv b \pmod m$

$a \cdot x_0 \equiv b \pmod m$

$\Rightarrow m \mid a \cdot x_0 - b \Rightarrow ax_0 - b = m \cdot y_0$ for some $y_0 \in \mathbb{Z}$.

$\Rightarrow b = ax_0 - my_0$

Let x is another solution ...

$b = a \cdot x - my$ for some $y \in \mathbb{Z}$

$0 = a(x_0 - x) - m(y_0 - y)$

$a(x_0 - x) = m(y_0 - y)$

divide by $d = \gcd(a, m)$

$\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

$\frac{a}{d}(x_0 - x) = \frac{m}{d}(y_0 - y)$

$\frac{m}{d} \mid \frac{a}{d}(x_0 - x) \Rightarrow \frac{m}{d} \mid (x_0 - x)$

$x = x_0 + \frac{m}{d} \cdot n, \quad n \in \mathbb{Z}$

Plug it into the equation

$ax = \underbrace{ax_0}_{\equiv b \pmod m} + a \cdot \underbrace{\frac{m}{d} \cdot n}_{\equiv 0 \pmod m, \ d \mid a} \equiv b \pmod m$

So far: $\{\text{solutions to } ax \equiv b \pmod m\} = \left\{ x_0 + \frac{m}{d} \cdot n \mid n \in \mathbb{Z} \right\}$

Find the incongruent ones

$x_0, \quad x_0 + \frac{m}{d}, \ \ldots, \ x_0 + \frac{m}{d}(d-1)$

it happens when $\frac{m}{d} \cdot n \equiv 0 \pmod m$

$m \mid \frac{m}{d} \cdot n \Rightarrow \frac{n}{d} \in \mathbb{Z}, \ d \mid n$

Say we have $x_0 + \frac{m}{d} \cdot k$, $x_0 + \frac{m}{d} n$ both are solutions $\pmod m$

When $x_0 + \frac{m}{d}k \equiv x_0 + \frac{m}{d}n \pmod m$?

$$\frac{m}{d}k \equiv \frac{m}{d}n \pmod m$$

$$\frac{m}{d}(k-n) \equiv 0 \pmod m \Rightarrow \frac{k-n}{d} \in \mathbb{Z}$$

$d \mid k-n$

$x_0,\ x_0+\frac{m}{d},\ x_0+\frac{m}{d}\cdot 2,\ \dots,\ x_0+\frac{m}{d}(d-1)$

$x_0+\frac{m}{d}\cdot d,\ x_0+\frac{m}{d}(d+1),\ \dots,\ x_0+m+\frac{m}{d}(d-1)$

Ex: $14x \equiv 21 \pmod{49}$

$\gcd(14,49) = 7$

$7 \mid 21 \Rightarrow$ there are solutions

$14 \cdot x_0 = 49 \cdot k + 21$

$x_0 = 5$

$k = 0, 1, \dots, 6$

$\frac{m}{d} = \frac{49}{7} = 7$ (7 congruency classes)

$\{5, 12, 19, 26, 33, 40, 47\}$

$5 + 49n,\ 12 + 49n,\ 19 + 49n,\ 26 + 49n,\ 33 + 49n,\ 40 + 49n,\ 47 + 49n$

Ex: $ax \equiv 1 \pmod m$ has a solution iff $\gcd(a,m) = 1$ and it is unique mod m

Def: Let $a, m \in \mathbb{Z}$, $m \neq 0$. The multiplicative inverse of a mod m is an integer $0 \leq b < m$ s.t. $a \cdot b \equiv 1 \pmod m$.

Chinese Remainder Theorem:

Eg example

- Split among 5 people evenly: # = 5, 10, 15, 20, 25, 30, 35, 40, 45
- Split between 3 people $\Rightarrow$ 2 left over

#, 5, 20, 35, ... 155, ...

— between 7 people ⇒ 1 left over

#, 155, ...

In other words, we solved the following system of linear congruences:

$$x \equiv 0 \pmod 5$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 7$$

Theorem (CRT): let $m_1, \dots, m_n \in \mathbb{Z}$, $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$

let $b_1 \dots b_n \in \mathbb{Z}$

Then the system

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv b_n \pmod{m_n}$$

has a unique solution $\pmod{m_1 \cdot m_2 \cdot \dots \cdot m_n}$.

Proof: 1) Construct a solution

let $M = m_1 \dots m_n$, $M_i = \frac{M}{m_i} = m_1 \dots \hat{m_i} \dots m_n$ ← missing

$\gcd(M_i, m_i) = 1$ because $\gcd(m_i, m_j) = 1$, $i \neq j$

$\Rightarrow M_i \cdot x_i \equiv 1 \pmod{m_i}$ has a solution since $\gcd(M_i, m_i) = 1$

Ex:

$$x \equiv 5 \pmod 7$$
$$x \equiv 1 \pmod{11}$$
$$x \equiv 2 \pmod 6$$

$M = 7 \cdot 11 \cdot 6 = 462$

$M_1 = 11 \cdot 6 = 66$	$M_2 = 7 \cdot 6 = 42$	$M_3 = 7 \cdot 11 = 77$
$m_1 = 7$	$m_2 = 11$	$m_3 = 6$
$b_1 = 5$	$b_2 = 1$	$b_3 = 2$
$M_1 \cdot x_1 \equiv 1 \pmod{m_1}$	$42 \cdot x_2 \equiv 1 \pmod{11}$	$77 x_3 \equiv 1 \pmod 6$
$66 \cdot x_1 \equiv 1 \pmod 7$	$9 \cdot x_2 \equiv 1 \pmod{11}$	$5 x_3 \equiv 1 \pmod 6$
$3 x_1 \equiv 1 \pmod 7$	$x_2 = 5$	$x_3 = 5$
$x_1 = 5$		

$a \equiv b \pmod c$

$c \equiv d \pmod c$

$ac \equiv bd \pmod c$

$$x = b_1 \cdot M_1 \cdot x_1 + b_2 \cdot M_2 \cdot x_2 + b_3 \cdot M_3 \cdot x_3$$
$$= 5 \cdot 66 \cdot 5 + 1 \cdot 42 \cdot 5 + 2 \cdot 77 \cdot 5 = 326 \pmod{462}$$

All solutions: $\{5 \cdot 66 \cdot 5 + 1 \cdot 42 \cdot 5 + 2 \cdot 77 \cdot 5 + 462 \cdot n\}$, $n \in \mathbb{Z}$

Cont'd: write $x = \underbrace{b_1 M_1 x_1}_{\equiv b_1 \pmod{m_1}} + \underbrace{b_2 M_2 x_2}_{\equiv b_2 \pmod{m_2}} + \dots + \underbrace{b_n M_n x_n}_{\equiv b_n \pmod{m_n}}$

Claim: x solves
$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

Indeed, $b_j M_j x_j \equiv 0 \pmod{m_i}$ $i \neq j$ because $m_i \mid M_j$

$\Rightarrow x \equiv b_i \underbrace{M_i x_i}_{\equiv 1 \pmod{m_i}} \pmod{m_i}$

$\Rightarrow x \equiv b_i \cdot 1 = b_i \pmod{m_i}$

2) prove uniqueness (mod M)

Let x' is another solution to the system

$\forall i$ $x' \equiv b_i \pmod{m_i}$

also $x \equiv b_i \pmod{m_i}$

$\Rightarrow x - x' \equiv 0 \pmod{m_i}$

$x \equiv x' \pmod{m_i}$

$\Rightarrow m_i \mid x - x'$ $\forall i$

$\Rightarrow M \mid x - x'$ $\Rightarrow x \equiv x' \pmod{M}$.

$\Rightarrow$ because $\gcd(m_i, m_j) = 1$, $i \neq j$

Ex:
$$\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod 6 \end{cases}$$

1, 12, 23 ... $\equiv 5 \pmod 7$

by CRT $x = 12$ is the unique solution to
$$\begin{aligned} x &\equiv 5 \pmod 7 \\ x &\equiv 1 \pmod{11} \end{aligned}$$
modulo $7 \cdot 11 = 77$

12, 12+77, 12+77·2, 12+77·3, ...

12, 89, 166, 243, 320, ...

$\{320 + 7 \cdot 11 \cdot 6 \cdot n \mid n \in \mathbb{Z}\}$

Wilson's theorem: Consider $(n-1)! = 1 \cdot 2 \cdot 3 \cdots (n-1) \pmod n$

$n=5$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \equiv 4 \pmod 5 \equiv -1 \pmod 5$

$n=7$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 6 \pmod 7 \equiv -1 \pmod 7$

$n=11$ $\quad \underbrace{1 \cdot 2 \cdot 3 \cdot 4}_{\equiv 2 \pmod{11}} \cdot \underbrace{5 \cdot 6 \cdot 7}_{\equiv 1 \pmod{11}} \cdot \underbrace{8 \cdot 9 \cdot 10}_{\equiv 5 \pmod{11}} \equiv 10 \pmod{11} \equiv -1 \pmod{11}$

$n=10$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 0 \pmod{10}$

$n=12$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 0 \pmod{12}$

Theorem: $(p-1)! \equiv -1 \pmod p$ iff p is prime.

Proof: ($\Rightarrow$) Suppose $n = a \cdot b$, $1 < a, b < n$

$a \mid (n-1)!$, $\quad a \mid n$

Suppose $(n-1)! \equiv -1 \pmod n$

$\Downarrow$

$n \mid (n-1)! + 1$

$a \mid n \mid ((n-1)!+1) \Rightarrow a \mid ((n-1)!+1)$ contradiction.

So $n = p \cdot$ prime.

($\Leftarrow$) $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv -1 \pmod 7$

%

Lemma: If p is a prime, $a \in \mathbb{Z}$ then $a^2 \equiv 1 \pmod p$ iff $a = \pm 1 \pmod p$

Proof: ($\Leftarrow$): If $a = \pm 1 \pmod p$

$a^2 = (\pm a)^2 \equiv 1 \pmod p$

($\Rightarrow$) Suppose $a^2 \equiv 1 \pmod p$

$a^2 - 1 \equiv 0 \pmod p$

$(a-1)(a+1) \equiv 0 \pmod p \Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid (a-1)$ or $p \mid (a+1)$

$\Downarrow$

$a \equiv 1 \pmod p$ $\quad a \equiv -1 \pmod p$

%

Back to Wilson:

$\Leftarrow$. $p=2$ then $(p-1)! = 1 \equiv -1 \pmod 2$

Ex $p=7$: $6! = 1\underbrace{(2\cdot 3)\cdot(4\cdot 5)}\cdot 6 \equiv -1 \pmod 7$, $\underbrace{(2\cdot 3)\cdot(4\cdot 5)} \equiv 1$

multiplicative inverses mod 7: $2\cdot 4 \equiv 1 \pmod 7$, $3\cdot 5 \equiv 1 \pmod 7$

• $p>2$

$(p-1)! = 1\cdot 2\cdot 3\cdot 4\cdot \ldots \cdot p-1$

pair each number $2 < a \le p-2$ with its multiplicative inverse.

Note that the multiplicative inverse is unique

$a \cdot b \equiv 1 \pmod c$

All factors will be paired up except $(p-1)$

which means that

$(p-1)! = 1\cdot 2\cdot 3 \cdots (p-2)(p-1) \equiv (p-1) \pmod p$

$\equiv 1 \pmod p$ $\qquad \equiv -1 \pmod p$.

Thm (Little Fermat Theorem)

if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

Ex: $3^{1600000} \equiv 4 \pmod 7$

Fermat: $3^6 \equiv 1 \pmod 7$

$(3^6)^2 \equiv 1 \pmod 7$

$(3^6)^n \equiv 1 \pmod 7$

$1600000 = 6\cdot n + 4$

$1600000 \equiv 4 \pmod 6$

$3^{1600000} = 3^{6\cdot n}\cdot 3^4 \equiv 1\cdot 3^4 = 81 \pmod 7 \equiv 4 \pmod 7$ (Fermat)

Ex: $3^{789} \equiv 3 \pmod 5$

FLT: $3^4 \equiv 1 \pmod 5$

$789 \equiv 1 \pmod 4$

$3^{789} = 3^{4\cdot 197}\cdot 3^1 = 3$

Ex: $7^{485} \equiv 11 \pmod{11}$

$7^{10} \equiv 1 \pmod{11}$

$7^{485} = 7^{48 \cdot 10} \cdot 7^5 \equiv 7^5 \pmod{11}$

$7^2 \equiv 5 \bmod 11$

$7^4 \equiv 25 \pmod{11} \equiv 3 \pmod{11}$

$7 \equiv 7 \pmod{11}$

$7^5 \equiv 21 \pmod{11} = 10 \bmod 11$

Thm (Little Fermat Theorem)
if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

Proof: $1, 2, 3, \ldots, p-1$ $\times a$

$a; 2a, 3a, \ldots (p-1)a$

Claim: $\{a, 2a, \ldots (p-1)a\}$ reduced modulo p is $\{1, 2, 3, \ldots p-1\}$ in some order

Ex: $p = 11$, $a = 3$

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ $\times 3$

$3, 6, 9, 12, 15, 18, 21, 24, 27, 30$

$\pmod{11}$

$3, 6, 9, 1, 4, 7, 10, 2, 5, 8$

In $\{a, 2a, \ldots (p-1)a\}$ no two elements are congruent mod p

if false: $ka \equiv \ell a \pmod{p}$

$(k-\ell) \cdot a \equiv 0 \pmod{p}$

let a^{-1} be the multiplicative inverse of $a \pmod{p}$

$(k-\ell) \cdot a \cdot a^{-1} \equiv 0 \pmod{p}$

$k - \ell \equiv 0 \pmod{p} \Rightarrow k \equiv \ell \pmod{p}$

$\Rightarrow k = \ell$.

So claim is true.

Consider product: $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) = a^{p-1} \cdot (p-1)!$

$\equiv -a^{p-1} \pmod p$ (Wilson)

By claim: $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$

$(p-1)! \equiv -1 \pmod p$ (Wilson)

Thus $-a^{p-1} \equiv -1 \pmod p$

or $a^{p-1} \equiv 1 \pmod p$.

Q: what if n is not prime → $p-1$ ($n = p$ is prime)

$a^{\#(n)} \equiv 1 \pmod n$

Ex: $n = 10$, $a = 3$

$a^1 \equiv 3 \pmod{10}$
$a^2 \equiv 9 \pmod{10}$
$a^3 \equiv 7$
$a^4 \equiv 1$
$a^5 \equiv 3$
$a^6 \equiv 9$
$a^7 \equiv 7$
$a^8 \equiv 1$
$a^9 \equiv 3$

$3^4 \equiv 1 \pmod{10}$

$\phi(10) = 4$

$1, 3, 7, 9$

$n = 15$, $a = 2$

$a^1 \equiv 2 \pmod{15}$
$a^2 \equiv 4$
$a^3 \equiv 8$
$a^4 \equiv 1$
$\vdots$
$a^8 \equiv 1 \pmod{15}$

$\phi(15) = 8$

$1, 2, 4, 7, 8, 11, 13, 14$

Theorem (Euler) Let $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod n$,

where $\phi(n)$ - Euler totient function - # positive integers $\leq n$ which are coprime with n.

Note: LFT: when $n = p$ - prime $\phi(p) = p - 1$

Proof: List all integers ≥ 0, $< n$ that are coprime with n

$u_1, u_2, \ldots, u_{\phi(n)}$ $\times a$

$au_1, au_2, \ldots, au_{\phi(n)}$

Claim: $\{u_1, u_2, \ldots, u_{\phi(n)}\} \equiv \{au_1, au_2, \ldots, au_{\phi(n)}\} \pmod n$

Ex. $n=15$, $n=2$

$\{1, 2, 4, 7, 8, 11, 13, 14\}_{\times 2}$

$2, 4, 8, 14, 16, 22, 26, 28$

$\equiv \pmod{15}$

$\{2, 4, 8, 14, 1, 7, 11, 13\}$

. . .

$a u_1 \cdot a u_2 \cdot \dots \cdot a u_{\varphi(n)} = a^{\varphi(n)} \underbrace{u_1 u_2 \dots u_{\varphi(n)}}_{K}$

By claim

$\equiv u_1 \cdot u_2 \dots u_{\varphi(n)} = K \pmod n$

K^{-1} exists because $\gcd(a, n) = 1$

so we can multiply by K^{-1}

$a^{\varphi(n)} \equiv 1 \pmod n$

Proof of the claim: $a u_1, \dots, a u_{\varphi(n)}$

$\gcd(a u_i, n) = 1$ (since $\gcd(a, n) = 1$, $\gcd(u_i, n) = 1$)

Let $a \cdot u_i = q \cdot n + r$ $\quad \gcd(r, n) = 1$

(from Euclid algorithm $\gcd(r, n) = \gcd(a u_i, n) = 1$)

Suppose $s \mid r$, $s \mid n \Rightarrow s \mid \underbrace{qn + r}_{a u_i} \Rightarrow s \mid a u_i$

So s is a common factor between $a u_i$ and n which is not possible

$\Rightarrow$ residue of $a u_i \pmod n$ is coprime with n.

Also $a u_i \equiv a u_j \pmod n$

$a^{-1} \cdot a u_i \equiv a^{-1} \cdot a u_j \pmod n$ $\quad a^{-1}$ exists since $\gcd(n, a) = 1$

$u_i \equiv u_j \pmod n \Rightarrow u_i = u_j$

The claim is proven.

Ex: $3^{500} \equiv 1 \pmod{20}$

Euler's theorem: $3^{\varphi(20)} \equiv 1 \pmod{20}$

$1, 3, 7, 9, 11, 13, 17, 19$

$\varphi(20) = 8$

$3^8 \equiv 1 \pmod{20}$

$500 \equiv 4 \pmod 8$

$3^{500} = 3^{8 \cdot 62} \cdot 3^4 \equiv 3^4 \pmod{20} \equiv 1 \pmod{20}$

Ex: $6^{500} \equiv 16 \pmod{20}$

$2^{500} \cdot 3^{500} \equiv 1 \pmod{20}$

$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8$
$2^4 \equiv 16$
$2^5 \equiv 12$
$2^6 \equiv 4$
$2^7 \equiv 8$
$2^8 \equiv 16$
$2^9 \equiv 12$
$2^{10} \equiv 4$

$2^{4k+2} \equiv 4 \pmod{20}$

$2^{498} \equiv 4 \pmod{20}$

$2^{500} \equiv 4 \cdot 2^2 = 16 \pmod{20}$

How to calculate $\varphi(n)$?

$\varphi(15) = 8$ $\quad$ $\varphi(20) = 8$

$15 = 3 \cdot 5$ $\quad$ $20 = 4 \cdot 5$

1, 7, 11, 13, 17, 19, 23, 29

$\varphi(30) = 8$ $\quad$ $\varphi(42) = 12$

$30 = 2 \cdot 3 \cdot 5$ $\quad$ $42 = 2 \cdot 3 \cdot 7$

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41

for primes $\varphi(p) = p-1$

$\varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

$\varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$

$\varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$

$\varphi(7) \cdot \varphi(3) \varphi(7) = 1 \cdot 2 \cdot 6 = 12$

Theorem: If $\gcd(m,n) = 1$ then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Corollary: Let $n = \underbrace{p_1^{q_1}}_{m} \cdot \underbrace{p_2^{q_2} \cdots p_k^{q_k}}_{n}$ is the prime factorization of n

then $\varphi(n) = \varphi(p_1^{q_1}) \varphi(p_2^{q_2}) \cdots \varphi(p_k^{q_k})$

Proof by iteration since $\gcd(p_1, p_2, \ldots p_k) = 1$, etc.

Q: What is $\varphi(p^k)$, p - prime, $k \geq 1$

Ex: $\varphi(3^3)$ $\quad$ $\varphi(27) = 18$

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26

Numbers ≤ 27 which are divisible by 3:

3, 6, 9, 12, 15, 18, 21, 24, 27 $\leftarrow$ 9 numbers

$27 - 9 = 18$

In general, if $\gcd(a, p^k) = 1 \iff p \nmid a$ $\quad \varphi(p^k)$

Divisible by p: $1\cdot p,\ 2\cdot p,\ 3\cdot p \dots,\ \underbrace{p^{k-1}\cdot p}_{p^k}$ there are p^{k-1} of them

$1, \dots, p^k$ — p^k numbers

There are $p^k - p^{k-1}$ numbers >0, $\le p^k$ that are not divisible by p and thus coprime with p^k.

So $\boxed{\varphi(p^k) = p^k - p^{k-1}}$

$16 = 2^4$

$2^4 - 2^3 = 8$

$\varphi(16) = 8$

By the corollary

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \dots \varphi(p_k^{a_k}) = \prod_{i=1}^{k} \left(p_i^{a_i} - p_i^{a_i - 1}\right)$$

Or, differently,

$$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i}\left(1 - \frac{1}{p_i}\right) = \left(\prod_{i=1}^{k} p_i^{a_i}\right) \cdot \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

($\prod_{i=1}^{k} p_i^{a_i} = n$)

% Notation $\quad a_1 \cdot a_2 \cdot \dots \cdot a_n = \prod_{i=1}^{n} a_i$ (prod)

$a_1 + \dots + a_n = \sum_{i=1}^{n} a_i$ %.

Ex: $\varphi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16$

$2^3 \cdot 5$ $\quad 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$

Ex: $\varphi(42) = 42\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 42 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$

$2 \cdot 3 \cdot 7$

Ex: $\varphi(7!) = \varphi(2^4 \cdot 3^2 \cdot 5 \cdot 7) = \varphi(2^4)\varphi(3^2) \cdot \varphi(5) \cdot \varphi(7)$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7$ $\quad = (2^4 - 2^3)(3^2 - 3^1) \cdot 4 \cdot 6$

$= 2^4 \cdot 3^2 \cdot 5 \cdot 7$ $\quad = 8 \cdot 6 \cdot 4 \cdot 6$

Th: If $\gcd(m, n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m)\varphi(n)$

Cryptography:

$A \mapsto B$

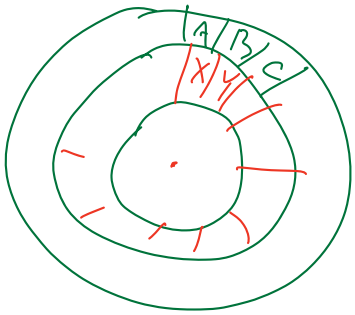
$B \mapsto A$

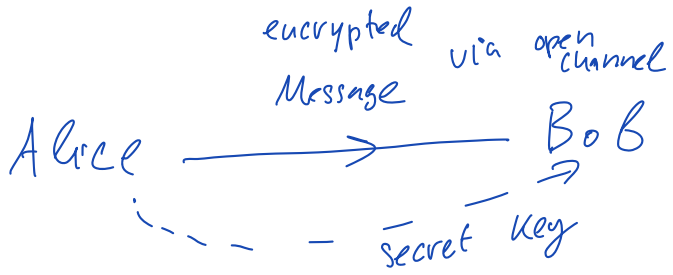
$A \mapsto X$

MATH

↓

NBVJ





RSA: prime factorization

1990 challenge to factor a 193-digit number

2005 - someone did it.

HEY, WE LOVE NUMBERS

A → 00

B → 01

⋮

Z → 25

22041419 . . .

$N = p \cdot q$ — primes

$\Phi(N) = \Phi(p)\,\Phi(q) = (p-1)(q-1)$

Let e be relatively prime to $\Phi(N)$

Solves: $e \cdot X \equiv 1 \pmod{\Phi(N)}$

Solution $X = r_1 \cdot C$, $r_1 = \frac{1}{\gcd(e, \Phi(N))} = 1$

$X = C$

$1 = e \cdot C + \Phi(N) \cdot D$, $D \in \mathbb{Z}$

Bob computes $x = e^{-1}$ - mult. inverse of e

e - public

e^{-1} - private

public

$e = 7$

$N = 35 = 7 \cdot 5$

$\Phi(N) = 6 \cdot 4 = 24$

HEY

07 04 24

$(07)^e = 7^7 \equiv 28 \pmod{35}$

$4^7 \equiv 4 \pmod{35}$

$24^7 \equiv 24 \pmod{35}$

$7 \cdot e^{-1} \equiv 1 \pmod{24}$

$e^{-1} = 7$

28 04 24

Bob

$28^{e^{-1}} = 28^7 \equiv 7 \pmod{35}$

$4^7 \equiv 4 \pmod{77}$

$24^7 \equiv 24 \pmod{30}$

07 04 24 → HEY

RSA: $N = 5 \cdot 7 = 35$

$\Phi(N) = 4 \cdot 6 = 24$

Open key (35, 7)

Message: 6 Coding $6^7 \equiv 6 \pmod{35}$

Secret key (35, 7) Decoding $6^7 \equiv 6 \pmod{35}$

$N = 11 \cdot 13 = 143$

$\Phi(N) = 120$ Open key (143, 23)

Message: 9 coding $9^{23} \equiv 3 \pmod{143}$

Secret key (143, 3) $3^3 \equiv 9 \pmod{143}$

C

RSA.

Alice $\xrightarrow{\quad e \quad}$ Bob

$m \mapsto m.m'$

$m.\text{hash}(m)$

Open key $(N = p \cdot q, \ e)$ — e is modulo invertible

Secret key $(\phi(N) = (p-1)(q-1))$

m - message (integer)

encryption by Alice: $c = m^e \pmod N$

She sends c to Bob via an open channel.

Bob receives c

decription: Bob computes $d = e^{-1}$ modulo $\phi(N)$

$d \cdot e \equiv 1 \pmod{\phi(N)}$

$d \cdot e = 1 + q\,\phi(N)$ for some $q \in \mathbb{Z}$

Next Bob takes

$$c^d \pmod N = (m^e)^d = m^{e \cdot d} \pmod N$$

$$= m^1 \cdot m^{q\phi(N)} \pmod N = m \cdot \underbrace{(m^{\phi(N)})^q}_{\| \ 1 \pmod N} \pmod N$$

$$\equiv m \pmod N$$

Ex: Message HEY

$07 \ 04 \ 24$

$m_1 = 7 \qquad c_1 = 7^7 \equiv 28 \pmod{35}$

$m_2 = 4 \qquad c_2 = 4^7 \equiv 4 \pmod{35}$

$m_3 = 24 \qquad c_3 = 24^7 \equiv 24 \pmod{35}$

$N = 35 \qquad p = 5, \ q = 7$

$\phi(N) = 4 \cdot 6 = 24$

$e = 7 \qquad 7 \cdot d \equiv 1 \pmod{24}$

$d = 7$

Open key: $(35, 7)$ — N, e

Secret key: $(24, 7)$ — $\phi(N)$, d

$$7^7 = (7^2)^3 \cdot 7 \equiv 14^3 \cdot 7 \equiv \underbrace{196}_{5 \cdot 35 + 21} \cdot 14 \cdot 7 \equiv 21 \cdot 14 \cdot 7 = 21 \cdot 98$$

$$\equiv 21 \cdot (-7)$$

$$\equiv -147 \equiv 28 \pmod{35}$$

$$4^7 = (4^3)^2 \cdot 4 \equiv (-6)^2 \cdot 4 \equiv 4 \pmod{35}$$

($4^3 = 64$, $64 \equiv -6 \pmod{35}$, $(-6)^2 = 36$, $36 \equiv 1 \pmod{35}$)

$$24^7 = 4^7 \cdot 6^7 \equiv 4 \cdot (6^2)^3 \cdot 6 \equiv 24 \pmod{35}$$

($6^2 \equiv 1 \pmod{35}$)

Bob gets 28 04 24

deciphering:

$$28^7 \equiv 4^7 \cdot 7^7 \equiv 4 \cdot 28 = 112 \equiv 7 \pmod{35}$$

$$4^7 \equiv 4 \pmod{35}$$

$$24^7 \equiv 24 \pmod{35}$$

07 04 24

↓

HEY

1) $A \xrightarrow{A} B$ same message every day

$e = 3$

$A^3 \equiv X \pmod{N_1}$ $\quad (N_1, e)$

$A^3 \equiv Y \pmod{N_2}$ $\quad (N_2, e)$

$A^3 \equiv Z \pmod{N_3}$ $\quad (N_3, e)$

CRT says that the system has a unique solution mod $N_1 N_2 N_3$

$A^3 < N_1 N_2 N_3$

Solve for A^3, take cube root, find A.

2) $N = pq$ if $q < p < 2q$, $d < \frac{N^{1/4}}{3}$

then it is relatively easy to find d.

Hints on 1:

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right)$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} \cdots\right)$$

$$\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \cdots\right)$$

$$\left(1 + \frac{1}{5^5} + \frac{1}{5^{75}} + \frac{1}{5^{175}} + \cdots\right)$$

$$\cdot$$

$$)$$

(2) $ax \equiv b \pmod m$ $\qquad d = \gcd(a, m)$

$\exists\, d$ incongruent solutions

a) $\gcd(40, 81) = 1$

b) $\gcd(51, 99) = 3$ — no inverse

$40 \cdot x \equiv 1 \pmod{81}$

$40 \cdot x = 1 + 81 \cdot q$

$\gcd(40, 81) = \underset{\text{"}}{1} = \underset{-2}{C} \cdot 40 + \underset{1}{D} \cdot 81 \quad = 1$

$X = k \cdot C = -2 \equiv 79 \pmod{81}$.

(6a) $n = p$ prime $\Rightarrow$ $(p-2)! \equiv 1 \pmod p$

$(p-1)! = (p-2)! \cdot (p-1) \pmod p$

$\equiv\!\equiv\!\equiv \quad \equiv\!\equiv\!\equiv \quad \equiv\!\equiv\!\equiv$

$-1 \qquad\quad 1 \qquad\quad -1$

$\Leftarrow$ Assume $(n-2)! \equiv 1 \pmod n$ show that n is prime.

Wilson $(n-1)! \equiv (-1) \pmod n$ iff n is prime

$(n-1)(n-1)! \equiv 1 - n \pmod n \equiv 1 \pmod n$

$\underbrace{(n-1)(n-1)}_{\equiv\!\equiv\!\equiv} \cdot (n-2)! \equiv 1 \pmod n$

$u^2 - 2u + 1 \pmod n$

$\equiv\!\equiv\!\equiv$

$1 \pmod n$

$(n-2)! \equiv 1 \pmod n$

iff n is prime

$$\prod_{p} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\text{-prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \cdots\right)$$

$$\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \cdots\right)$$

$$\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^{3s}} + \cdots\right)$$

$$\left(1 + \frac{1}{7^s} + \cdots\right)$$

$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{2^s \cdot 3^s \cdot 5^s \cdots} + \cdots$$

$$= \frac{1}{2^{k_1 s} \cdot 3^{k_2 s} \cdot 5^{k_3 s} \cdots} \qquad k_1, k_2, k_3, \ldots \in \mathbb{Z}$$

prime decomposition on all n.

$$\rightarrow \left(2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdots\right)^{-s}$$

n

($\Rightarrow$) $\quad x \equiv b_1 \pmod{m_1}$

$x \equiv b_2 \pmod{m_2}$

$x = b_1 + m_1 \cdot k \qquad x = b_2 + m_2 \cdot \ell$

$b_1 + m_1 \cdot k = b_2 + m_2 \cdot \ell$

$b_1 - b_2 = m_2 \ell - m_1 k$

$\gcd(m_1, m_2) \mid m_1, m_2 \Rightarrow \gcd(m_1, m_2) \mid b_1 - b_2$

($\Leftarrow$) $\quad$ Let $\gcd(m_1, m_2) \mid b_1 - b_2$

$b_1 - b_2 = K \cdot \gcd(m_1, m_2)$

$= K(X \cdot m_1 + Y \cdot m_2)$

$= KX m_1 + KY m_2$

$b_1 = KX m_1 + KY m_2 + b_2 \equiv KX m_1 + b_2 \pmod{m_2}$

$b_1 \equiv K Y m_2 + b_2 \pmod{m_1}$

$b_2 \equiv b_1 - k_1 m_2 \pmod{m_1}$

$x \equiv b_1 \pmod{m_1}$

$x \equiv b_2 \pmod{m_2}$