Quick Summary

Congruence mod m

Modular Arithmetic

Modular Inverse

- Solving a linear congruence

Arithmetic with very large integers

- Solving system of linear congruences
- Chinese Remainder Theorem

Modular Arithmetic Calculations

What is $rem(999 + 376, 7)$?

Recall: $a \equiv b \ (mod\ m) \ \wedge \ c \equiv d \ (mod\ m) \implies a + c \equiv b + d \ (mod\ m)$

$$999 \equiv rem(999,7) \equiv 5 \quad (mod\ 7)$$
$$376 \equiv rem(376,7) \equiv 5 \quad (mod\ 7)$$
$$999 + 376 \equiv 5 + 5 \equiv 3 \quad (mod\ 7)$$

Similarly:

$$999 \times 376 \equiv 5 \times 5 \equiv 4 \quad (mod\ 7)$$

Furthermore:

$$999 + (999 + 376)^2 + 376^2$$
$$\equiv 5 + 3^2 + 5^2 \quad (mod\ 7)$$
$$\equiv 5 + 2 + 4 \ (mod\ 7)$$
$$\equiv 4 \ (mod\ 7)$$

Moral: Keep reducing numbers to their class representative in $\mathbb{Z}_m$

Computing with Large Integers

Modular Arithmetic

- Convert large integer into a k-tuple of remainders modulo k pairwise relative primes
- Perform modular arithmetic operations on each element in the k-tuple separately
- Convert the resulting k-tuple into a large integer to obtain the final result
    - Chinese Remainder Theorem

This worked for addition and multiplication. What about exponentiation?

What is $7^{222}\ (mod\ 11)$?

Fermat's Little Theorem

Theorem. If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \ (mod\ p)$.

Example: $p = 5, a = 7$

$$7^4 \equiv 7^2 \cdot 7^2 \equiv 49 \cdot 49 \equiv 4 \cdot 4 \equiv 1 \ (mod\ 5)$$

Example: What is $rem(7^{222}, 11)$?

$$\begin{aligned} 7^{222} &= 7^{(10 \cdot 22+2)} \\ &\equiv (7^{10})^{22} \cdot 7^2 \ \ (mod\ 11) \\ &\equiv 1^{22} \cdot 49 \ \ (mod\ 11) \\ &\equiv 5 \ (mod\ 11) \end{aligned}$$

Fermat's Little Theorem

Theorem. If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \ (mod\ p)$.

Idea: When $p = 7$ and $a = 10$ consider the set

$\{10i: \ 1 \leq i \leq 6\}$ (first 6 multiples of 10)

$= \{10, \ 20, \ 30, \ 40, \ 50, \ 60\}$

$\equiv \{3, \ 6, \ 2, \ 5, \ 1, \ 4\} \ (mod\ 7)$

(abusing notation: the numbers in the two sets are congruent)

So: $(10 \cdot 20 \cdot 30 \cdot 40 \cdot 50 \cdot 60) \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \ (mod\ 7)$

$\Rightarrow 10^6(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \ (mod\ 7)$

$\Rightarrow 10^6 \equiv 1 \ (mod\ 7) \quad since \ \gcd(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6, 7) = 1$

Fermat's Little Theorem

Theorem. If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \ (mod\ p)$.

Proof: Consider the numbers $1a,\ \ 2a,\ \ 3a, \dots, (p-1)a$

1. None of these numbers is congruent to 0 modulo p.
2. Note that for all i, j in $[1, p-1]$, $\ i \neq j \ \Rightarrow \ p \nmid (i-j)$
   Since $\ p \nmid a$ it follows that $\quad i \neq j \Rightarrow \ p \nmid (i-j)a$
   $\Rightarrow \ \ ia \not\equiv ja \ \ (mod\ p)$

From 1 and 2 it follows that $\{1a,\ \ 2a,\ \ 3a, \dots, (p-1)a\} \equiv \{1,2, \dots, p-1\}\ (mod\ p)$

Therefore, $1a \times 2a \times \cdots \times (p-1)a \ \equiv 1 \times 2 \times \cdots \times (p-1)\ (mod\ p)$

Rearranging the LHS: $\ 1 \times 2 \times \cdots \times (p-1) \times a^{p-1} \equiv 1 \times 2 \times \cdots \times (p-1) \ \ (mod\ p)$

Because $\gcd\big(p, 1 \times 2 \times \cdots \times (p-1)\big) = 1$ we can cancel the common factor to get:

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

Euler's Totient Function

Definition: Euler's totient function $\phi(n) =$ number of numbers in $[1, n]$ relatively prime to n.

Example:

$$\phi(1) = 1$$
$$\phi(6) = 2$$
$$\phi(17) = 16$$

Lemma:

1) If p is prime, then $\phi(p) = p - 1$.
2) If p, q are primes then $\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$

In general, if $p_1, p_2, \ldots, p_k$ are the prime divisors of n, then

$$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_k)$$

Example: $\phi(300) = 300 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) = 80$

Euler's Generalization of Fermat's Little Theorem

Theorem. If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \ (mod\ n)$

Example:

$n = 300,\ a = 49$

$\gcd(300,49) = 1$

$\phi(n) = 80$

Therefore, $49^{80} \equiv 1 \ (mod\ 300)$

Euler's Generalization of Fermat's Little Theorem

Theorem. If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \ (mod\ n)$

Proof. Let $k_1, k_2, \ldots, k_{\phi(n)}$ be the numbers in $[1, n]$ relatively prime to n.

Consider the numbers $ak_1, ak_2, \ldots, ak_{\phi(n)}$

1. Each of these is relatively prime to n.
2. No two of them are congruent to each other $mod\ n$.

Therefore, $\{ak_1, ak_2, \ldots, ak_{\phi(n)}\} = \{k_1, k_2, \ldots, k_{\phi(n)}\}$

This implies that

$$ak_1 \times ak_2 \times \cdots \times ak_{\phi(n)} \equiv k_1 \times k_2 \times \cdots \times k_{\phi(n)} \ (mod\ n)$$

Rearranging the LHS: $k_1 \times k_2 \times \cdots \times k_{\phi(n)} \times a^{\phi(n)} \equiv k_1 \times k_2 \times \cdots \times k_{\phi(n)} (mod\ n)$

Because $\gcd\left(n, k_1 \times k_2 \times \cdots \times k_{\phi(n)}\right) = 1$ we can cancel the common factor to get:

$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

Securing Communication Channels

Alice wants to send a message m to Bob

Evil Eve is eavesdropping on the communication

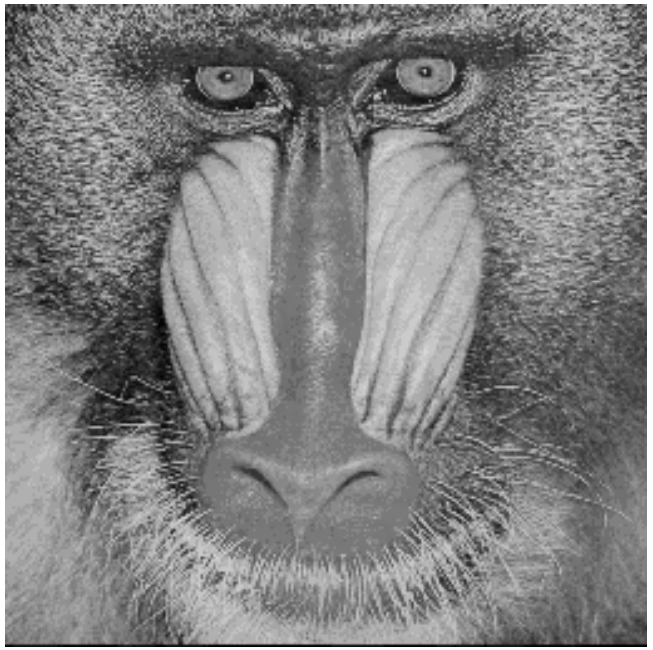
Eve can read every bit transmitted between Alice and Bob

Eve can send a that Bob will think it came from Alice (spoofing)

Eve can intercept and alter messages between Alice and Bob (man-in-the-middle)

How can Alice and Bob communicate securely even when Eve can read every bit transmitted?

Security by Obscurity



Transmit an innocuous message so Eve doesn't realize a secret is being transmitted.
When system security depends on the secrecy of the algorithm,
the system is compromised forever when the algorithm is discovered.

- Even in military situations, equipment is captured or bought
- CSS for DVD, RIAA digital watermarking, Adobe e-books, SDMI

Cryptography

Scramble the plaintext so that the ciphertext can be decoded quickly using the ***secret*** keys.

Example: Caesar Cipher (100 BC) Shift each alphabet letter k positions (mod 26)
Alice and Bob share the secret key k in advance.

Caesar(IBM, -1) = HAL Caesar(Hello, 5) = Mjqqt

Question: Decipher the Caesar encrypted ciphertext: DRSCSCDBSFSKVDYMBKMU

Need to figure out the secret key – only 26 possibilities. Pretty easy to decode without the key!

Crypto Hall of Shame

The Register®
Biting the hand that feeds IT

Bootnotes

Mafia boss undone by clumsy crypto

Little Caesar

By John Leyden 19 Apr 2006 at 14:14 SHARE ▼

Clues left in the clumsily encrypted notes of a Mafia don have helped Italian investigators to track his associates and ultimately contributed to his capture after years on the run.

The recently busted Bernardo Provenzano, reputed to be the "boss of bosses" of the Sicilian Mafia, used a modified form of the Caesar cipher to obscure "sensitive information" in notes left to either his family or underlings.

According to a biography (written by Italian journalists Salvo Palazzolo and Ernesto Oliva) on bernardoprovenzano.net, the content of these notes varied from meal requests to his family to orders to his lieutenants where numbers were used to disguise people's names.

Provenzano, 73, was arrested last week in a farm close to his home town of Corleone on the Italian island of Sicily after almost 40 years on the run. He's accused of numerous homicides including the 1992 murder of two judges, a crime that earned him a life sentence in absentia. Provenzano who earned the nickname Binnu u tratturi (Binnu the tractor) because of his rep for mowing down enemies, latterly took to writing instructions incorporating basic encryption on small scraps of paper, known locally as pizzini.

Most read


They forked this one up: Microsoft modifies open-source code, blows hole in Windows Defender


Intel admits a load of its CPUs have Spectre v2 flaw that can't be fixed


Cloudflare touts privacy-friendly 1.1.1.1 public DNS service. Hmm, let's take a closer look at that


Furious gunwoman opens fire at YouTube HQ, three people shot


'Every little helps'... unless you want email: Tesco to kill free service

"Looks like kindergarten cryptography to me. It will keep your kid sister out, but it won't keep the police out. But what do you expect from someone who is computer illiterate?"

… security guru Bruce Schneier.

Substitution Ciphers

Substitute each letter of the alphabet by a unique letter.

Choose a bijection $S: \{a, b, \dots, z\} \to \{a, b, c, \dots z\}$

How many bijections?

Choose $f(a)$: 26 choices

$f(b)$: 25 choices

$f(c)$: 24 choices …

Total # bijections = $26 \cdot 25 \cdot 24 \cdot \cdots 2 \cdot 1 \approx 11^{26}$

LQ IXPQ DQQK MVGEMYFFQD XUXVK

20th century encryption devices

Enigma

The German Enigma Machine

Breaking the Enigma

During WWII all branches of the German military used the Enigma for communications.

The keys were changed each day: over 15×10^{18} possible settings!

An early model of the Enigma was mistakenly mailed to Poland

Poland, since an earlier war with Russia, had a team of expert codebreakers

On the eve of WWII the Polish shared their knowledge with British codebreakers

Under the guidance of Alan Turing, the British developed a machine “Bombe” to break Enigma

Analysis made possible by flaws in how the Germans used Enigma

Bombe used to learn positions of German U-Boats in advance

Turing died in 1954, but his contributions to the war were kept secret until 1974.

More on Alan Turing

Turing's Bombe