Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

Imdad ullah Khan

Congruence

Definition

For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, $\quad a \equiv_m b \quad \text{iff} \quad m \mid (a - b)$

Theorem

For $a, b \in \mathbb{Z}$ *and* $m \in \mathbb{Z}^+$, $\quad a \equiv_m b \quad \textit{iff} \quad a \,\%\, m = b \,\%\, m$

Theorem

For $a, b \in \mathbb{Z}$ *and* $m \in \mathbb{Z}^+$, $\quad a \equiv_m b \iff \exists\, k \in \mathbb{Z} : a = b + km$

Modular Arithmetic

Lemma

If $a \equiv_m b$ *and* $c \equiv_m d$, *then* $a + c \equiv_m b + d$

▷ $8 \equiv_5 3$ and $9 \equiv_5 4 \implies 8 + 9 \equiv_5 3 + 4$

Familiar cases: $m = 2$ **and** $m = 10$

If (a, b) and (c, d) have the same parity, then $a + c$ and $b + d$ have the same parity

If (a, b) and (c, d) have the same last digit, then $a + c$ and $b + d$ have the same last digit

The lemma says it works for all m

Modular Arithmetic

Lemma

If $a \equiv_m b$ *and* $c \equiv_m d$, *then* $a + c \equiv_m b + d$

Proof:

$a \equiv_m b \implies a = b + xm$ AND

$c \equiv_m d \implies c = d + ym$

$a + c = b + d + xm + ym \implies (a + c) - (b + d) = m(x + y)$

Hence $m \mid (a + c) - (b + d)$

So $a + c \equiv_m b + d$

Modular Arithmetic

Lemma

If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$

Proof:

Very similar!

Lemma

If $a \equiv_m b$, then $a^k \equiv_m b^k$

Proof:

Very similar!

Modular Arithmetic

Lemma

1. *If* $a \equiv_m b$ *and* $c \equiv_m d$, *then* $a + c \equiv_m b + d$
2. *If* $a \equiv_m b$ *and* $c \equiv_m d$, *then* $ac \equiv_m bd$
3. *If* $a \equiv_m b$, *then* $a^k \equiv_m b^k$

Corollary

1. $(a + b) \,\%\, m = \big((a \,\%\, m) + (b \,\%\, m)\big) \,\%\, m$
2. $ab \,\%\, m = \big((a \,\%\, m)(b \,\%\, m)\big) \,\%\, m$
3. $a^k \,\%\, m = \big(a \,\%\, m\big)^k \,\%\, m$

This means that while computing $(a + c) \,\%\, m$ or $(ac) \,\%\, m$, we can replace a with $(a \,\%\, m)$ and c with $(c \,\%\, m)$ ▷ Recall that $a \equiv_m a \,\%\, m$

Modular Arithmetic

Lemma

1. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$
2. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$
3. If $a \equiv_m b$, then $a^k \equiv_m b^k$

Corollary

1. $(a + b) \% m = ((a \% m) + (b \% m)) \% m$
2. $ab \% m = ((a \% m)(b \% m)) \% m$
3. $a^k \% m = (a \% m)^k \% m$

Compute $-706 \cdot 1456 \% 19$

$-706 \equiv_{19} 16$ and $1456 \equiv_{19} 12 \implies -706 \cdot 1456 \% 19 = 16 \cdot 12 \% 19$

Modular Arithmetic

Lemma

1. *If* $a \equiv_m b$ *and* $c \equiv_m d$, *then* $a + c \equiv_m b + d$
2. *If* $a \equiv_m b$ *and* $c \equiv_m d$, *then* $ac \equiv_m bd$
3. *If* $a \equiv_m b$, *then* $a^k \equiv_m b^k$

Corollary

1. $(a + b) \,\%\, m = \big((a \,\%\, m) + (b \,\%\, m)\big) \,\%\, m$
2. $ab \,\%\, m = \big((a \,\%\, m)(b \,\%\, m)\big) \,\%\, m$
3. $a^k \,\%\, m = (a \,\%\, m)^k \,\%\, m$

$A = \{-706, 1456, 88, -41, 19, 20, 38, 40\}$ Compute $\left(\sum_{x \in A} x\right) \% \, 19$

Remainders: $R = \{16, 12, 12, 16, 0, 1, 0, 2\}$ So $\left(\sum_{x \in A} x\right) \% \, 19 = \left(\sum_{r \in R} r\right) \% \, 19$

Modular Arithmetic

Lemma

1. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$
2. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$
3. If $a \equiv_m b$, then $a^k \equiv_m b^k$

Corollary

1. $(a + b) \,\%\, m = ((a \,\%\, m) + (b \,\%\, m)) \,\%\, m$
2. $ab \,\%\, m = ((a \,\%\, m)(b \,\%\, m)) \,\%\, m$
3. $a^k \,\%\, m = (a \,\%\, m)^k \,\%\, m$

Compute $516^{3031} \,\%\, 103$

$516 \equiv_{103} 1$ So $516^{3031} \,\%\, 103 = 1^{3031} \,\%\, 103 = 1$

Modular Arithmetic: Applications

Theorem

A positive integer N is divisible by 9 iff the sum of its digits is divisible by 9

$9 \mid 343233153711$

because $9 \mid 3+4+3+2+3+3+1+5+3+7$

$9 \nmid 12356954236$

because $9 \nmid 1+2+3+5+6+9+5+4+2+3+6$

Modular Arithmetic: Applications

Theorem

A positive integer N is divisible by 9 iff the sum of its digits is divisible by 9

Proof: Note that $10 \equiv_9 1$

Let $N = d_k d_{k-1} \dots d_2 d_1 d_0$ $\triangleright$ d_i : i^{th} digit of N

$$N = d_k 10^k + d_{k-1} 10^{k-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 10^0$$

Using the congruence identities

$$N \equiv_9 d_k 10^k + \dots + d_2 10^2 + d_1 10^1 + d_0 10^0$$

$$N \equiv_9 d_k 1^k + \dots + d_2 1^2 + d_1 1^1 + d_0 1^0$$

$$N \equiv_9 d_k + d_{k-1} + \dots + d_2 + d_1 + d_0$$

Modular Arithmetic: Applications

Theorem

A positive integer N is divisible by 3 iff the sum of its digits is divisible by 3

Proof: Essentially the same

Modular Arithmetic: Applications

Theorem

A positive integer N is divisible by 11 iff the alternating sum of its digits is divisible by 11

Proof: Essentially the same, using the fact that $10 \equiv_{11} -1$

Modular Arithmetic: Applications

Definition (Check Digit)

An extra digit appended to a number, which is related to the other digits in some way

Airlines Tickets

12 digits ticket number, plus a 13^{th} check digit

check digit is the main number % 7

01-1300696717-2 as 11300696717 % 7 = 2

▷ Catches most transposition and single-digit errors

Modular Arithmetic: Applications

Definition (Check Digit)

An extra digit appended to a number, which is related to the other digits in some way

Airlines Tickets

12 digits ticket number, plus a 13^{th} check digit

Difficult to find check digit by most calculators

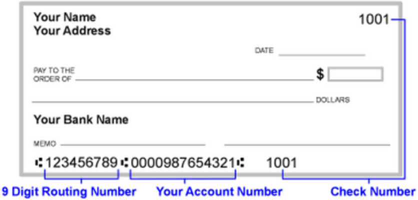
Easier to compute using modular arithmetic

Modular Arithmetic: Applications

Definition (Check Digit)

An extra digit appended to a number, which is related to the other digits in some way

Bank routing transit number



Banks have 9 digits routing numbers. $d_8 d_7 \ldots d_3 d_2 d_1 d_0$

$d_0 = 7d_8 + 3d_7 + 9d_6 + 7d_5 + 3d_4 + 9d_3 + 7d_2 + 3d_1 \ \% \ 10$

▷ Catches single-digit and most transposition errors

Modular Exponentiation

Given (large) integers b, m, n

Find $b^n \ \% \ m$

Compute $2851^{3177} \ \% \ 4559$

2851^{3177} has about $12k$ digits!

Modular Exponentiation

Find $22^4 \% 29$

Notice that we can take % after each multiplication

$22^4 \% 29 = 22 \cdot 22 \cdot 22 \cdot 22 \% 29$

$= 22 \cdot 22 \cdot 484 \% 29 = 22 \cdot 22 \cdot 20 \% 29$

$= 22 \cdot 440 \% 29 = 22 \cdot 5 \% 29 = 110 \% 29 = 23$

It helps for the number of digits (storage) but number of steps is still large