MODULAR ARITHMETIC

BEGIN WITH A BRIEF SYNOPSIS OF A FEW OF THE MOST ELEMENTARY NOTIONS FROM NUMBER THEORY.

$$\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$$

$a, b \in \mathbb{Z}$, $a \neq 0$: a DIVIDES b $(a|b) \iff \exists\, q \in \mathbb{Z}$ s.t. $b = qa$

E.G., $-4 \mid 36$ $(36 = (-9)(-4))$

$a, b \in \mathbb{Z}$, NOT BOTH 0 : (a,b) = GREATEST COMMON DIVISOR OF a AND b

= THE UNIQUE INTEGER d S.T.

(i) $d|a$ AND $d|b$

(ii) $c|a$ AND $c|b \Rightarrow c \leq d$

a, b RELATIVELY PRIME $\iff (a,b) = 1$

E.G., $(-52, 39) = 13$ AND $(8, 27) = 1$

DIVISION ALGORITHM : $a, b \in \mathbb{Z}$, $a > 0$, $b > 0 \Rightarrow \exists!\, q, r \in \mathbb{Z}$ WITH $0 \leq r < b$ S.T.

$$a = qb + r$$

COROLLARY : $(a,b) = (b,r)$

EUCLIDEAN ALGORITHM :

$$(a,b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-1}, 0) = r_n$$

$a = q_0 b + r_0$ $\quad$ $b = q_1 r_0 + r_1$

$0 \leq r_0 < b$ $\quad$ $0 \leq r_1 < r_0 < b$

E.G.,

$$(299, 247) = (247, 52) = (52, 39) = (39, 13) = (13, 0) = 13$$

$299 = 1 \cdot 247 + 52$ $\quad$ $247 = 4 \cdot 52 + 39$ $\quad$ $52 = 1 \cdot 39 + 13$ $\quad$ $39 = 3 \cdot 13 + 0$

REVERSING THE STEPS IN THE EUCLIDEAN ALGORITHM GIVES

$$a, b \in \mathbb{Z}, \text{ NOT BOTH } 0 \Rightarrow \exists\, x, y \in \mathbb{Z} \text{ s.t. } (a,b) = ax + by$$

E.G.,

$$\begin{aligned}(299, 247) = 13 &= 52 - 1 \cdot 39 \\ &= 52 - 1 \cdot (247 - 4 \cdot 52) \\ &= 5 \cdot 52 - 1 \cdot 247 = 5 \cdot (299 - 1 \cdot 247) - 1 \cdot 247 \\ &= 299 \cdot 5 + 247 \cdot (-6)\end{aligned}$$

COROLLARIES :

$$d \mid ab \text{ AND } (d, a) = 1 \Rightarrow d \mid b$$

$$a \mid n \text{ AND } b \mid n \text{ AND } (a, b) = 1 \Rightarrow ab \mid n$$

THE EQUATION $ax + by = c$ HAS INTEGER SOLUTIONS $\Leftrightarrow (a, b) \mid c$

UNIQUE FACTORIZATION THEOREM : EVERY INTEGER $n > 1$ CAN BE WRITTEN IN EXACTLY ONE WAY IN THE FORM

$$n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$$

WHERE $p_1 < p_2 < \cdots < p_k$ ARE PRIMES AND $i_1, i_2, \ldots, i_k$ ARE POSITIVE INTEGERS.

$a, b, m \in \mathbb{Z}$, $m > 0$:

a IS CONGRUENT TO b MODULO m ($a \equiv b \bmod m$) $\iff$ $m \mid a-b$

$\iff$ $a = b + km$, SOME $k \in \mathbb{Z}$

$\iff$ a, b HAVE THE SAME REMAINDER WHEN DIVIDED BY m

E.G., $49 \equiv 9 \bmod 10$, $111 \equiv 3 \bmod 4$, $27 \equiv 0 \bmod 3$

> EVERY a IS CONGRUENT MOD m TO PRECISELY ONE OF
>
> $0, 1, \ldots, m-1$
>
> (ITS REMAINDER ON DIVISION BY m ; CALLED THE LEAST RESIDUE OF a MOD m)

EQUIVALENCE RELATION :

$a \equiv a \bmod m$

$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$

$a \equiv b \bmod m$ AND $b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$

$[a]$ = CONGRUENCE CLASS OF a MOD m

$= \{ a + km : k \in \mathbb{Z} \}$

PROPERTIES :

$a \equiv b \bmod m$ AND $c \equiv d \bmod m \Rightarrow a+c \equiv (b+d) \bmod m$ AND $ac \equiv bd \bmod m$

$ac \equiv bc \bmod m \Rightarrow a \equiv b \bmod \left(\frac{m}{(c,m)} \right)$

DIGITS : $n \in \mathbb{Z}$, $n \geq 0$: $n = d_k d_{k-1} \cdots d_1 d_0$ (DIGITS, NOT A PRODUCT)

MEANS

$$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10^1 + d_0$$

E.G., $832 = 8 \cdot 10^2 + 3 \cdot 10^1 + 2$

LAST DIGIT (d_0) = LEAST RESIDUE OF n MOD 10

LAST TWO DIGITS ($d_1 d_0$) = LEAST RESIDUE OF n MOD 100

ETC.

E.G., TO FIND THE LAST DIGIT OF 7^{355} NOTE THAT $7^4 = 49 \cdot 49 \equiv 1$ MOD 10 SO

$$7^{355} = 7^{4 \cdot 83 + 3} = (7^4)^{83} 7^3 \equiv 1^{83} 7^3 \text{ MOD } 10$$

$$\equiv 7^3 \text{ MOD } 10 \equiv 343 \text{ MOD } 10 \equiv 3 \text{ MOD } 10$$

SO THE LAST DIGIT IS 3.

DIVISIBILITY TRICKS : $10^k \equiv 1$ MOD 9 $\forall k \Rightarrow$

ANY n IS CONGRUENT MOD 9 TO THE SUM OF ITS DIGITS.

E.G., 10,352,106 IS DIVISIBLE BY 9 BECAUSE

$$1+0+3+5+2+1+0+6 = 18 \equiv 0 \text{ MOD } 9$$

SIMILARLY,

ANY n IS CONGRUENT MOD 3 TO THE SUM OF ITS DIGITS.

AND

ANY n IS CONGRUENT MOD 11 TO THE ALTERNATING SUM OF ITS DIGITS.

QUADRATIC RESIDUES :

ANY a IS CONGRUENT MOD 10 TO ONE OF $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$

SO ANY SQUARE IS CONGRUENT MOD 10 TO ONE OF $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 6$, $5^2 \equiv 5$, $6^2 \equiv 6$, $7^2 \equiv 9$, $8^2 \equiv 6$, $9^2 \equiv 1$.

$$\{0, 1, 4, 5, 6, 9\}$$

ARE THE QUADRATIC RESIDUES MOD 10.

E.G., NO PERFECT SQUARE CAN END IN 2, 3, 7, OR 8

(SO 87,953,128 IS NOT A SQUARE)

SINCE $0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \bmod 4$, $2^2 \equiv 0 \bmod 4$, $3^2 \equiv 1 \bmod 4$, THE QUADRATIC RESIDUES MOD 4 ARE $\{0, 1\}$.

E.G., NONE OF THE NUMBERS

$$11, 111, 1111, 11111, \ldots$$

IS A PERFECT SQUARE BECAUSE

$$\begin{aligned} \underbrace{11\ldots11}_{k} &= 1 + 10 + 10^2 + \cdots + 10^{k-1} \\ &\equiv 1 + 2 + 2^2 + \cdots + 2^{k-1} \bmod 4 \\ &\equiv \frac{2^k - 1}{2-1} \bmod 4 \equiv (2^k - 1) \bmod 4 \\ &\equiv -1 \bmod 4 \quad (k \geq 2) \\ &\equiv 3 \bmod 4 \end{aligned}$$

SOME NONTRIVIAL (BUT USEFUL) RESULTS ON CONGRUENCES:

1. (FERMAT'S LITTLE THEOREM) p PRIME AND $(a,p)=1 \Rightarrow$

$$a^{p-1} \equiv 1 \bmod p$$

2. (EULER'S THEOREM) n POSITIVE INTEGER AND $(a,n)=1 \Rightarrow$

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

WHERE

$\varphi(n)$ = NUMBER OF POSITIVE INTEGERS $\leq n$ THAT ARE RELATIVELY PRIME TO n (EULER φ-FUNCTION)

3. (WILSON'S THEOREM) p PRIME $\iff (p-1)! \equiv -1 \bmod p$

4. (CHINESE REMAINDER THEOREM) IF $m_1, \ldots, m_k$ ARE PAIRWISE RELATIVELY PRIME ($(m_i, m_j) = 1$ IF $i \neq j$) AND $a_1, \ldots, a_k$ ARE ARBITRARY INTEGERS, THEN $\exists$ INTEGER X SUCH THAT

$$\begin{aligned} X &\equiv a_1 \bmod m_1 \\ X &\equiv a_2 \bmod m_2 \\ &\vdots \\ X &\equiv a_k \bmod m_k \end{aligned}$$

EXAMPLES:

1. SELECT 55 NUMBERS FROM THE SET $\{1, 2, \ldots, 99, 100\}$. PROVE THAT, AMONG THESE 55 NUMBERS, THERE MUST BE AT LEAST TWO THAT DIFFER BY 9.

EVERY ELEMENT OF $\{1,2,\ldots,99,100\}$ IS CONGRUENT MOD 9 TO ONE OF $0, 1, \ldots, 8$ (9 CONGRUENCE CLASSES / PIGEONHOLES), I.E., IS OF THE FORM

$9k$	$k = 1,\ldots,11$	(11 NUMBERS)
$9k+1$	$k = 0,\ldots,11$	(12 NUMBERS)
$9k+2$	$k = 0,\ldots,10$	(11 NUMBERS)
$9k+3$	$k = 0,\ldots,10$	"
$9k+4$	$k = 0,\ldots,10$	"
$9k+5$	$k = 0,\ldots,10$	"
$9k+6$	$k = 0,\ldots,10$	"
$9k+7$	$k = 0,\ldots,10$	"
$9k+8$	$k = 0,\ldots,10$	"

THERE ARE $55 = 6\cdot 9 + 1$ NUMBERS / PIGEONS SO AT LEAST 7 OF THE NUMBERS MUST APPEAR IN THE SAME CLASS, SAY,

$$9k_1 + \ell, \ \ldots, \ 9k_7 + \ell$$

WHERE $k_1 < \cdots < k_7$. WE CLAIM THAT, FOR SOME $i = 1,\ldots,6$, $k_{i+1} = k_i + 1$. IF NOT, THEN $k_{i+1} - k_i \geq 2 \ \forall i = 1,\ldots,6$ SO

$$k_7 - k_1 = (k_7 - k_6) + (k_6 - k_5) + \cdots + (k_2 - k_1) \geq 6\cdot 2 = 12$$

AND THIS IS IMPOSSIBLE SINCE THE MAXIMUM DIFFERENCE BETWEEN TWO k-VALUES IN EITHER $1,\ldots,11$, $0,\ldots,11$, OR $0,\ldots,10$ IS 11. NOW,

$$(9k_{i+1} + \ell) - (9k_i + \ell) = (9k_i + 9 + \ell) - (9k_i + \ell) = 9$$

SO $9k_{i+1} + \ell$ AND $9k_i + \ell$ DIFFER BY 9.

2. SHOW THAT $2^{70} + 3^{70}$ IS DIVISIBLE BY 13.

NOTE THAT $3^3 = 27 \equiv 1 \bmod 13$ SO

$$3^{70} = 3^{3\cdot 23+1} = (3^3)^{23}\cdot 3 \equiv 1^{23}\cdot 3 \bmod 13 \equiv 3 \bmod 13$$

AND

$$2^{12} \equiv 1 \bmod 13 \quad \text{(FERMAT'S LITTLE THEOREM)}$$

SO

$$2^{70} = 2^{5\cdot 12+10} = (2^{12})^5 \cdot 2^{10} \bmod 13 \equiv 2^{10} \bmod 13$$

$$\equiv (2^5)^2 \bmod 13 \equiv 32^2 \bmod 13 \equiv 6^2 \bmod 13 \equiv 36 \bmod 13$$

$$\equiv 10 \bmod 13.$$

THUS,

$$2^{70} + 3^{70} \equiv (10+3) \bmod 13 \equiv 0 \bmod 13.$$

3. DO THERE EXIST 1,000,000 CONSECUTIVE INTEGERS EACH OF WHICH CONTAINS AT LEAST ONE REPEATED PRIME FACTOR?

THE ANSWER IS "YES". IN FACT, 1,000,000 CAN BE REPLACED BY ANY POSITIVE INTEGER k. TO SEE THIS, LET

$$P_1, \ldots, P_k$$

BE A SET OF k DISTINCT PRIMES (THERE ARE INFINITELY MANY PRIMES SO WE CAN CHOOSE AS MANY AS WE LIKE). THEN

p_i^2 AND p_j^2 ARE RELATIVELY PRIME IF $i \neq j$. THE CHINESE REMAINDER THEOREM IMPLIES THAT THERE IS AN INTEGER X SUCH THAT

$$\begin{aligned} X &\equiv -1 \bmod p_1^2 \\ X &\equiv -2 \bmod p_2^2 \\ &\vdots \\ X &\equiv -k \bmod p_k^2 \end{aligned}$$

SO $p_1^2 \mid X+1$, $p_2^2 \mid X+2$, ..., $p_k^2 \mid X+k$. THUS,

$$X+1, X+2, \ldots, X+k$$

IS A SEQUENCE OF k CONSECUTIVE INTEGERS EACH OF WHICH HAS A REPEATED PRIME FACTOR.

A FEW FACTS WORTH REMEMBERING:

FOR INTEGERS $n \geq k \geq 0$,

$\binom{n}{k}$ = "n CHOOSE k" = NUMBER OF WAYS TO SELECT k OBJECTS FROM A SET OF n OBJECTS

$$= \frac{n!}{k!\,(n-k)!}$$

BINOMIAL THEOREM: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

IDENTITIES:

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} \qquad (k \geq 1)$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \text{(PASCAL'S TRIANGLE)}$$

$$\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{n+m}{k}$$