IF $k+1$ IS PRIME, THEN THERE IS NOTHING MORE TO PROVE. IF NOT, THEN IT IS COMPOSITE: $\exists$ INTEGERS $b, c \ni 1 < b \leq c < k+1$ AND $k+1 = bc$. BY HYPOTHESIS, $b = p_1 p_2 \cdots p_j$ AND $c = q_1 q_2 \cdots q_m$ ARE PRODUCTS OF PRIMES.

THEN $k+1 = bc = p_1 p_2 \cdots p_j q_1 q_2 \cdots q_m$ IS A PRODUCT OF PRIMES. ✓

$\therefore$ EVERY $a \in \mathbb{N} \setminus \{1\}$ IS EITHER PRIME OR A PRODUCT OF PRIMES.

NOW WE SHOW UNIQUENESS, BY CONTRADICTION. ASSUME THAT $a > 1$ IS THE PRODUCT OF PRIMES IN TWO DIFFERENT WAYS:

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

SINCE $p_1 | a$, EUCLID'S LEMMA SAYS p_1 DIVIDES ONE OF THE q_j. WITHOUT LOSS OF GENERALITY, LET $p_1 | q_1$. SINCE q_1 IS PRIME, ITS DIVISORS ARE 1 AND q_1. HENCE, $p_1 = q_1$, AND

$$\frac{a}{p_1} = p_2 p_3 \cdots p_m = q_2 q_3 \cdots q_n.$$

BY THE SAME LOGIC, p_2 MUST DIVIDE ONE OF THE REMAINING q_j, WLOG $p_2 | q_2$.

THEN

$$\frac{a}{p_1 p_2} = p_3 p_4 \cdots p_m = q_3 q_4 \cdots q_n.$$

CONTINUING LIKE THIS, WE FIND THAT $m \leq n$ AND $p_i = q_i \ \forall i \in \{1, 2, \ldots, m\}$. THE SAME ARGUMENT WITH THE p PRIMES AND q PRIMES REVERSED GIVES US THAT $n \leq m$ AND $q_i = p_i \ \forall i \in \{1, 2, \ldots, n\}$. THEREFORE, $m = n$ AND WE HAVE THAT THE TWO FACTORIZATIONS ARE THE SAME. $\square$

<u>EX</u>: FIND THE PRIME FACTORIZATION.

a) 924 b) 1300 c) 2722 d) 50,193

a) $924 = 2 \cdot 462 = 2^2 \cdot 231 = 2^2 \cdot 3 \cdot 77 = 2^2 \cdot 3 \cdot 7 \cdot 11$

b) $1300 = 2 \cdot 650 = 2^2 \cdot 325 = 2^2 \cdot 5 \cdot 65 = 2^2 \cdot 5^2 \cdot 13$

c) $2722 = 2 \cdot 1361$

d) $50{,}193 = 3 \cdot 16{,}731 = 3^2 \cdot 5577 = 3^3 \cdot 1859 = 3^3 \cdot 11 \cdot 169 = 3^3 \cdot 11 \cdot 13^2$

GREATEST COMMON DIVISOR (GCD)

DEF: LET $a, b \in \mathbb{Z}$ WITH AT LEAST ONE OF a, b NONZERO. THE GREATEST COMMON DIVISOR OF a AND b, DENOTED BY $\gcd(a,b)$, IS THE NUMBER $c \in \mathbb{N}$ SUCH THAT

a) c IS A COMMON DIVISOR OF a AND b: $c \mid a$ AND $c \mid b$;

b) IF d IS A COMMON DIVISOR OF a AND b, THEN $d \leq c$.

EX: $\gcd(18, 12) = 6$, SINCE $6 \mid 18$ AND $6 \mid 12$, AND THERE IS NO BIGGER INTEGER THAT DIVIDES THEM BOTH.

NOTE THAT $\gcd(18,12) = \gcd(-18,12) = \gcd(18,-12) = \gcd(-18,-12)$.

PRIME FACTORIZATIONS CAN BE USED TO FIND GCDs. IF $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ AND $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (SOME α_i, β_i CAN BE ZERO), THEN

$$\gcd(a,b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}, \text{ WHERE } \gamma_i = \min\{\alpha_i, \beta_i\}.$$

EX: GIVEN THAT $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ AND $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, WE HAVE

$$\gcd(3220, 1155) = 5 \cdot 7 = \boxed{35}$$

EX: FIND $\gcd(35{,}100, 6975)$

LEAST COMMON MULTIPLES (LCM)

DEF: LET $a, b \in \mathbb{Z}$ WITH AT LEAST ONE OF a, b NONZERO. THE LEAST COMMON MULTIPLE OF a AND b, DENOTED BY $\text{lcm}(a,b)$, IS THE NUMBER $c \in \mathbb{N}$ SUCH THAT

1) c IS A COMMON MULTIPLE OF a AND b; i.e., $a \mid c$ AND $b \mid c$;
2) IF d IS A COMMON MULTIPLE OF a AND b, THEN $c \le d$.

EX: a) $\text{lcm}(12, 4) = 12$

b) $\text{lcm}(18, 15) = 90$

WE CAN USE PRIME FACTORIZATION TO CALCULATE LCM. IF $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ AND $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (SOME α_i, β_i CAN BE ZERO), THEN

$$\text{lcm}(a,b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}, \text{ WHERE } \gamma_i = \max\{\alpha_i, \beta_i\}.$$

EX: GIVEN THAT $3220 = 2^2 \cdot 5 \cdot 7 \cdot 23$ AND $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, WE HAVE

$$\text{lcm}(3220, 1155) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 106{,}260$$

EXERCISE: FIND $\text{lcm}(35100, 6975)$.
FIND $\gcd(268944, 198466)$.

THE EUCLIDEAN ALGORITHM

THE EUCLIDEAN ALGORITHM IS A PROCESS FOR FINDING GCD. IT WORKS BECAUSE OF THE QUOTIENT-REMAINDER THEOREM AND THE FOLLOWING TWO LEMMAS.

LEMMA 1: FOR ALL $r \in \mathbb{N}$, $\gcd(r, 0) = r$.

PROOF: EXERCISE.

LEMMA 2: LET $a, b \in \mathbb{Z}$, $b \neq 0$, $q, r \in \mathbb{N} \ni a = bq + r$. THEN
$$\gcd(a,b) = \gcd(b,r).$$

PROOF: LET $D = \{d \in \mathbb{Z} : d \mid a, d \mid b\}$, $\overline{D} = \{d \in \mathbb{Z} : d \mid b, d \mid r\}$. WE WILL SHOW THAT $D = \overline{D}$.

$(\subseteq)$: LET $x \in D$. THEN $x \mid a$ AND $x \mid b$. WE HAVE

$$a = bq + r$$
$$\Rightarrow a - bq = r$$
$$\Rightarrow \frac{a - bq}{x} = \frac{r}{x}$$
$$\Rightarrow \frac{a}{x} - \frac{bq}{x} = \frac{r}{x}.$$

SINCE $\frac{a}{x}$ AND $\frac{bq}{x}$ ARE INTEGERS, WE HAVE $\frac{r}{x} \in \mathbb{Z}$, SO $x \mid r$.

HENCE, $x \in \overline{D}$, AND WE HAVE $D \subseteq \overline{D}$.

$(\supseteq)$: LET $x \in \overline{D}$. THEN $x \mid b$ AND $x \mid r$. WE HAVE

$$a = bq + r$$
$$\frac{a}{x} = \frac{bq + r}{x}$$
$$\frac{a}{x} = \frac{bq}{x} + \frac{r}{x}.$$

SINCE $\frac{bq}{x}$ AND $\frac{r}{x}$ ARE INTEGERS, WE HAVE $\frac{a}{x} \in \mathbb{Z}$, SO $x \mid a$.

HENCE, $x \in D$, AND WE HAVE $\overline{D} \subseteq D$.

THEREFORE, $D = \overline{D}$. SO EVERY COMMON DIVISOR OF a AND b IS ALSO A COMMON DIVISOR OF b AND r, AND VICE VERSA.

$$\therefore \gcd(a,b) = \max_{d \in D} d = \max_{d \in \overline{D}} d = \gcd(b,r). \qquad \square$$

EUCLIDEAN ALGORITHM:

1) LET $a < b \leq 0$.

2) CHECK IF $b = 0$. IF SO, LEMMA 1 SAYS $\gcd(a,b) = a$.

3) IF $b \neq 0$, USE QUOTIENT-REMAINDER THEOREM TO FIND q, r WITH $0 \leq r < b$ SUCH THAT $a = bq + r$. LEMMA 2 SAYS $\gcd(a,b) = \gcd(b,r)$.

4) SET $a = b$, $b = r$ AND GO TO STEP 2.

THIS ALGORITHM WILL TERMINATE WITH $r = 0$, SINCE EACH REMAINDER IS SMALLER THAN THE PREVIOUS ONE.

EX: FIND $\gcd(2772, 2310)$

$2772 = 2310 \cdot 1 + 462$

$2310 = 462 \cdot 5 + 0$

$\therefore \gcd(2772, 2310) = 462$.

EX: FIND $\gcd(-243, 223)$

$243 = 223 \cdot 1 + 20$ (REMEMBER $\gcd(a,b) = \gcd(|a|, |b|)$).

$223 = 20 \cdot 11 + 3$

$20 = 3 \cdot 6 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\therefore \gcd(-243, 223) = 1$.

DEF: INTEGERS a, b ARE CALLED COPRIME (RELATIVELY PRIME, MUTUALLY PRIME) IF $\gcd(a,b) = 1$.

<u>EXERCISE</u>: TRUE OR FALSE? FOR ALL $x \in \mathbb{N}$ THERE EXISTS $y \in \mathbb{N}$ SUCH THAT $\gcd(x,y) = 1$.

<u>THM (BÉZOUT'S IDENTITY)</u>: LET $a, b \in \mathbb{Z} \setminus \{0\}$. THEN $d = \gcd(a,b)$ EXISTS, AND THERE EXIST $m, n \in \mathbb{Z}$ SUCH THAT $ma + nb = d$.

<u>COROLLARY</u>: IF a AND b ARE RELATIVELY PRIME, THEN THERE EXIST $m, n \in \mathbb{Z}$ SUCH THAT $ma + nb = 1$.

HOW DO WE FIND m, n? WE USE THE EUCLIDEAN ALGORITHM IN REVERSE.

<u>EX</u>: FIND $m, n \in \mathbb{Z}$ SUCH THAT $\gcd(330, 156) = 330m + 156n$.

① $330 = 156 \cdot 2 + 18$

② $156 = 18 \cdot 8 + 12$

③ $18 = 12 \cdot 1 + 6$

④ $12 = 6 \cdot 2 + 0 \Rightarrow \gcd(330, 156) = 6$.

NOW STARTING WITH THE SECOND-LAST LINE, ISOLATE THE GCD AND USE EACH PREVIOUS LINE TO SUBSTITUTE FOR THE OTHER FACTORS.

③ $18 = 12 \cdot 1 + 6 \Rightarrow 6 = 18 - 12$

② $12 = 156 - 18 \cdot 8 \Rightarrow 6 = 18 - (156 - 18 \cdot 8) = -156 + 18 \cdot 9$

① $18 = 330 - 156 \cdot 2 \Rightarrow 6 = -156 + (330 - 156 \cdot 2) \cdot 9 = \boxed{330 \cdot 9 - 156 \cdot 19}$

$\therefore m = 9, n = -19$.

EX: FIND $m, n \in \mathbb{Z}$ SUCH THAT $243m + 223n = 1$.

$$243 = 223 \cdot 1 + 20$$
$$223 = 20 \cdot 11 + 3$$
$$20 = 3 \cdot 6 + 2$$
$$3 = 2 \cdot 1 + 1$$

$$\Rightarrow 1 = 3 - 2$$
$$= 3 - (20 - 3 \cdot 6) = -20 + 3 \cdot 7$$
$$= -20 + (223 - 20 \cdot 11) \cdot 7 = 223 \cdot 7 - 20 \cdot 78$$
$$= 223 \cdot 7 - (243 - 223) \cdot 78 = -243 \cdot 78 + 223 \cdot 85$$

$\therefore m = -78, n = 85$.

THE PIGEONHOLE PRINCIPLE: LET $k, n \in \mathbb{N}$, $k < n$. IF n PIGEONS FLY INTO k PIGEONHOLES, THEN SOME PIGEONHOLE CONTAINS AT LEAST TWO PIGEONS.

PROOF: SUPPOSE THAT EACH PIGEONHOLE CONTAINS AT MOST ONE PIGEON. THEN THE TOTAL NUMBER OF PIGEONS IS AT MOST $\sum_{i=1}^{k} 1 = k < n$, A CONTRADICTION. THEREFORE, THERE EXISTS A PIGEONHOLE THAT CONTAINS MORE THAN ONE PIGEON. $\square$

EXAMPLES:

a) YOU HAVE A DRAWER FULL OF SOCKS, OF 3 DIFFERENT COLOURS. HOW MANY SOCKS MUST YOU PICK AT RANDOM TO BE SURE YOU HAVE A MATCHING PAIR?

A: 4. THE FIRST 3 COULD POSSIBLY BE ALL 3 DIFFERENT COLOURS, BUT THE FOURTH WILL MATCH ONE OF THOSE (OR ELSE THERE'S A PREVIOUS PAIR).

b) IN A ROOM OF 367 PEOPLE (ALLOWING FOR LEAP YEAR), AT LEAST 2 OF THEM SHARE A BIRTHDAY.

c) HUMANS HAVE A MAXIMUM OF ABOUT 500,000 HAIRS. IS IT GUARANTEED THAT 2 RESIDENTS OF WOLLONGONG HAVE EXACTLY THE SAME NUMBER OF HAIRS? HOW ABOUT 2 RESIDENTS OF SYDNEY?

SOME FORMAL EQUIVALENT STATEMENTS TO THE PIGEONHOLE PRINCIPLE:

1) LET A BE A SET OF n ELEMENTS. IF A IS PARTITIONED INTO k PAIRWISE DISJOINT SUBSETS, WHERE $k < n$, THEN AT LEAST ONE SUBSET CONTAINS MORE THAN ONE ELEMENT.

2) A FUNCTION FROM ONE FINITE SET TO A SMALLER SET CANNOT BE ONE-TO-ONE. THERE MUST BE AT LEAST TWO ELEMENTS THAT MAP TO THE SAME POINT.

<u>Ex:</u> IN A GROUP OF 700 PEOPLE, MUST THERE BE TWO WHOSE FIRST NAMES HAVE THE SAME FIRST AND LAST LETTERS?

A: AT MOST 26 PEOPLE CAN HAVE DIFFERENT FIRST LETTERS, AND AT MOST 26 PEOPLE CAN HAVE DIFFERENT LAST LETTERS. SO AT MOST $26 \cdot 26 = 676$ PEOPLE CAN HAVE DIFFERENT <u>EITHER FIRST OR LAST</u> LETTERS. SO YES, A GROUP OF 700 HAS 2 THAT SHARE THE SAME FIRST AND LAST LETTERS.

PROBLEMS OF THIS SORT INVOLVE FIGURING OUT HOW TO FORM THE PIGEONHOLES PROPERLY (HOW TO PARTITION THE SET).

<u>EX:</u> 5 DIFFERENT NUMBERS ARE SELECTED FROM THE SET $S = \{1,2,3,4,5,6,7,8\}$. SHOW THAT 2 OF THE SELECTED NUMBERS SUM TO 9.

A: PARTITION THE SET INTO PAIRS THAT SUM TO 9 (THE PIGEONHOLES):

$S = \{1,8\} \cup \{2,7\} \cup \{3,6\} \cup \{4,5\}$. THERE ARE 4 SUBSETS, SO IT'S POSSIBLE TO SELECT 4 NUMBERS FROM S SUCH THAT ONLY ONE OF THEM BELONGS TO EACH SUBSET. CHOOSING 5 NUMBERS, BY THE PIGEONHOLE PRINCIPLE, RESULTS IN 2 NUMBERS CHOSEN BELONGING TO THE SAME SUBSET. $\square$

<u>EX:</u> A RESTAURANT SERVES 3 DIFFERENT SALADS, 6 DIFFERENT MAINS AND 4 DIFFERENT DESSERTS. HOW MANY PEOPLE MUST EAT THERE TO ENSURE THAT AT LEAST 2 OF THEM HAVE THE SAME MEAL.

A: THERE ARE $3 \cdot 6 \cdot 4$ DIFFERENT MEALS (THIS IS COMBINATORICS, MORE ON THIS LATER), SO THERE MUST BE 73 PEOPLE.

<u>GENERALIZED PIGEONHOLE PRINCIPLE</u>: IF n PIGEONS FLY INTO k PIGEONHOLES, AND $n > km$ FOR SOME $m \in \mathbb{N}$, THEN SOME PIGEONHOLE CONTAINS AT LEAST $m+1$ PIGEONS.

<u>EX:</u> SHOW THAT IN A GROUP OF 85 PEOPLE, THE FIRST NAME OF AT LEAST 4 OF THEM MUST START WITH THE SAME LETTER.

A: 85 PIGEONS, 26 PIGEONHOLES, $85 = 26 \cdot 3 + 7$. SO

$85 > 26 \cdot 3 \Rightarrow m = 3$, AND SOME PIGEONHOLE CONTAINS AT LEAST

$m+1 = 4$ PIGEONS.

$\therefore$ AT LEAST 4 PEOPLE'S NAMES START WITH THE SAME LETTER.

EXERCISE: FIND THE MINIMUM NUMBER OF STUDENTS IN A CLASS TO BE SURE 3 OF THEM ARE BORN IN THE SAME MONTH.

EX: WE WANT TO ASSIGN 70 STUDENTS TO 11 CLASSES SO THAT NO CLASS HAS MORE THAN 15 PEOPLE. SHOW THAT THERE MUST BE AT LEAST 3 CLASSES WITH 5 OR MORE PEOPLE.

A: ASSUME ONLY 2 CLASSES HAVE 5 OR MORE PEOPLE, AND SHOW A CONTRADICTION.

THE BEST CASE IS THAT THOSE 2 CLASSES ARE FULL (LEAVING THE FEWEST POSSIBLE PEOPLE FOR THE OTHER CLASSES), 15 STUDENTS EACH. THEN 40 PEOPLE REMAIN, FOR 9 CLASSES. SINCE

$40 = 9 \cdot 4 + 4$, $m = 4$ AND THE PRINCIPLE SAYS AT LEAST ONE OF THE 9 CLASSES HAS 5 PEOPLE OR MORE IN IT. $\square$

MODULAR ARITHMETIC

DEF: LET $n \in \mathbb{N}$, $a \in \mathbb{Z}$. WE DEFINE $a \bmod n$ TO BE THE REMAINDER WHEN a IS DIVIDED BY n.

EX:

$10 \bmod 4 = 2$ (SINCE $\frac{10}{4} = 2$ WITH REMAINDER 2)

$18 \bmod 3 = 0$

$-8 \bmod 6 = 4$

$10 \bmod 1 = 0$

DEF: a, b ARE <u>CONGRUENT MODULO n</u>, WRITTEN $a \equiv b \pmod{n}$, IF $n \mid (a-b)$. EQUIVALENTLY, $a \equiv b \pmod{n}$ IFF $a \bmod n = b \bmod n$.

EX: TRUE OR FALSE? a) $154 \equiv 56 \pmod{11}$ b) $7 \equiv -9 \pmod{8}$

a) $11 \mid (154-56) \Leftrightarrow 11 \mid 98$ FALSE.

b) $8 \mid (7-(-9)) \Leftrightarrow 8 \mid 16$ TRUE.

EX: FIND x SUCH THAT $12 \equiv x \pmod{5}$.

WE NEED $5 \mid (12-x)$, SO x IS ANY OF $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$

EXERCISE: IF $m \equiv 0 \pmod{2}$, WHAT CAN YOU SAY ABOUT m?

THM (CONGRUENCE ARITHMETIC): LET $n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$.

IF $a \equiv c \pmod{n}$ AND $b \equiv d \pmod{n}$, THEN

(1) $(a+b) \equiv (c+d) \pmod{n}$;

(2) $(a-b) \equiv (c-d) \pmod{n}$;

(3) $ab \equiv cd \pmod{n}$;

(4) $a^m \equiv c^m \pmod{n} \ \forall m \in \mathbb{N}$.

PROOF: $n \mid (a-c) \Rightarrow \boxed{a-c = np}, \ p \in \mathbb{Z}$.

$n \mid (b-d) \Rightarrow \boxed{b-d = nq}, \ q \in \mathbb{Z}$.

(1) $a+b = (np+c)+(nq+d) = n(p+q)+c+d$

$(a+b) \pmod{n} \equiv [\underbrace{n(p+q)}_{\to 0}+c+d] \pmod{n} \equiv (c+d) \pmod{n}$

(2) $a-b=(np+c)-(nq+d)=n(p-q)+(c-d)$

$$(a-b)(\text{mod}\,n)\equiv[\cancelto{0}{n(p-q)}+(c-d)](\text{mod}\,n)\equiv(c-d)(\text{mod}\,n)$$

(3) $ab=(np+c)(nq+d)=n^2pq+npd+nqc+cd=n(npq+pd+qc)+cd$

$$ab(\text{mod}\,n)\equiv[\cancelto{0}{n(npq+pd+qc)}+cd](\text{mod}\,n)\equiv cd(\text{mod}\,n)$$

(4) INDUCTION.

a) $m=1$: $a^1\equiv c^1(\text{mod}\,n)$ ✓

b) SUPPOSE $a^k\equiv c^k(\text{mod}\,n)$. PROVE $a^{k+1}\equiv c^{k+1}(\text{mod}\,n)$

$a^{k+1}=a^k\cdot a$ AND $c^{k+1}=c^k\cdot c$, SO BY (3), $a^k\cdot a\equiv c^k\cdot c\,(\text{mod}\,n)$

$\Rightarrow a^{k+1}\equiv c^{k+1}(\text{mod}\,n)$. ✓

$\therefore\ a^m\equiv c^m\,(\text{mod}\,n)\ \forall m\in\mathbb{N}$. $\square$

__EX__: a) GIVEN THAT $2064=1715+349$, FIND $2064\,(\text{mod}\,17)$.

b) GIVEN THAT $713064=803\cdot 888$, FIND $713064\,(\text{mod}\,8)$.

c) FIND x SUCH THAT $3^9\equiv x\,(\text{mod}\,5)$.

a) $1715\equiv 15\,(\text{mod}\,17)$ AND $349\equiv 9\,(\text{mod}\,17)$

$\Rightarrow(1715+349)\equiv(15+9)(\text{mod}\,17)\equiv 7\,(\text{mod}\,17)$.

b) $803\equiv 3\,(\text{mod}\,8)$ AND $888\equiv 0\,(\text{mod}\,8)$

$\Rightarrow 803\cdot 888\equiv 3\cdot 0\,(\text{mod}\,8)\equiv 0\,(\text{mod}\,8)$.

c) $3^9=3^4\cdot 3^4\cdot 3=81\cdot 81\cdot 3$. $81\equiv 1\,(\text{mod}\,5)$

$\Rightarrow 81\cdot 81\cdot 3\,(\text{mod}\,5)\equiv 1\cdot 1\cdot 3\,(\text{mod}\,5)\equiv 3\,(\text{mod}\,5)$.

EXERCISE: FIND THE REMAINDER WHEN 7^5 IS DIVIDED BY 16.

THM (CANCELLATION LAW): LET $n \in \mathbb{Z}$, $a, b, c \in \mathbb{Z}$. IF $\gcd(a,n) = 1$ ★ AND $ab \equiv ac \pmod{n}$, THEN $b \equiv c \pmod{n}$.

PROOF:

$$ab \equiv ac \pmod{n}$$

$$(ab - ac) \equiv 0 \pmod{n}$$

$$a(b-c) \equiv 0 \pmod{n}$$

$\Rightarrow a(b-c) = kn$ FOR SOME $k \in \mathbb{Z}$. BUT a AND n ARE COPRIME BY ★, SO THE FACTOR OF n ON THE LEFT-HAND SIDE IS CONTAINED IN $(b-c)$. HENCE,

$$(b-c) \equiv 0 \pmod{n}$$

$$b \equiv c \pmod{n} \qquad \square$$

NOTE: ★ IS ESSENTIAL. COUNTEREXAMPLE:

$$60 \equiv 90 \pmod{15}$$

$$10 \cdot 6 \equiv 10 \cdot 9 \pmod{15}, \text{ BUT}$$

$$6 \not\equiv 9 \pmod{15}.$$

SINCE 10 AND 15 ARE NOT COPRIME, THE CANCELLATION LAW DOES NOT APPLY.

EX: GIVEN $10904 \equiv 32 \pmod 9$, FIND THE SMALLEST $x \in \mathbb{N}$ SUCH THAT $x \equiv 1363 \pmod 9$.

A: NOTE THAT $10904 = 1363 \cdot 8$.

$1363 \cdot 8 \equiv 4 \cdot 8 \pmod 9$

$1363 \equiv 4 \pmod 9$ (SINCE 8 & 9 ARE COPRIME)

$\therefore x = 4$. ($4 < 9$, SO THERE CAN BE NO SMALLER CONGRUENCE TO.)

CONGRUENCE CLASSES MODULO n

THE QUOTIENT-REMAINDER THEOREM GIVES US THE FOLLOWING.

FACT: LET $n \in \mathbb{Z}$. EVERY INTEGER $x \in \mathbb{Z}$ IS CONGRUENT MODULO n TO EXACTLY ONE ELEMENT IN $\{0, 1, 2, \ldots, n-1\}$.

THIS ALLOWS US TO GROUP INTEGERS ACCORDING TO THEIR REMAINDERS AFTER DIVIDING BY n.

DEF: LET $n \in \mathbb{N}$. THE CONGRUENCE CLASS (RESIDUE) OF $a \in \mathbb{Z}$ MODULO n IS THE SET $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod n\}$.

EX: WRITE THE CONGRUENCE CLASSES FOR $n = 4$. HOW MANY OF THEM ARE THERE?

THM: LET $n \in \mathbb{N}$. THERE ARE EXACTLY n DISTINCT CONGRUENCE CLASSES: $[0], [1], \ldots, [n-1]$.

PROOF: FIRST, SHOW THAT NO TWO OF $0, 1, \ldots, n-1$ ARE CONGRUENT MODULO n. LET $0 \le a < b < n$, $a, b \in \mathbb{N}$. THEN $b-a \in \mathbb{N}$ AND $b-a < n$. THUS, $n \nmid (b-a)$, SO $b \not\equiv a \pmod{n}$. THEREFORE, NO TWO OF $0, 1, \ldots, n-1$ ARE CONGRUENT, AND WE HAVE THAT $[0], [1], \ldots, [n-1]$ ARE ALL DISTINCT RESIDUES.

NEXT, SHOW THAT EVERY $x \in \mathbb{Z}$ IS IN ONE OF THESE RESIDUES. THE QUOTIENT-REMAINDER THEOREM GIVES $x = nq + r$, $0 \le r < n$. SO $r \in \{0, 1, \ldots, n-1\}$, AND $x - r = nq \Rightarrow x \equiv r \pmod{n}$. THEREFORE, EVERY $x \in \mathbb{Z}$ IS IN ONE OF $[0], [1], \ldots, [n-1]$. $\square$

DEF: LET $n \in \mathbb{N}$. THE COMPLETE SET OF RESIDUES MODULO n IS THE SET

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

EX: $\mathbb{Z}_3 = \{[0], [1], [2]\}$, SO IN $\mathbb{Z}_3$, WE HAVE

$$[4] = [1]; \quad [-1] = [2]; \quad [30] = [0].$$

EX: IN $\mathbb{Z}_n$,

a) $[0] \cup [1] \cup \cdots \cup [n-1] =$

b) $[0] \cap [1] \cap \cdots \cap [n-1] =$

OPERATIONS ON $\mathbb{Z}_n$

WE WANT TO DEFINE ADDITION AND MULTIPLICATION ON $\mathbb{Z}_n$. SINCE DIFFERENT NUMBERS CAN GIVE THE SAME RESIDUES, WE MUST BE CAREFUL WITH THE DEFINITIONS.

<u>THM</u>: LET $n \in \mathbb{N}$. THE OPERATION $+$:

$$[a]+[b]=[a+b]$$

IS WELL-DEFINED ADDITION ON $\mathbb{Z}_n$, i.e. IF $[a]=[c]$ AND $[b]=[d]$, THEN $[a+b]=[c+d]$. SIMILARLY, THE OPERATION $\cdot$:

$$[a][b]=[ab]$$

IS WELL-DEFINED MULTIPLICATION ON $\mathbb{Z}_n$, i.e. IF $[a]=[c]$ AND $[b]=[d]$, THEN $[ab]=[cd]$.

<u>PROOF</u>:

$[a]=[c] \Rightarrow a \equiv c \pmod{n} \Rightarrow \exists\, k_1 \in \mathbb{Z} \ni a = c+k_1 n.$

$[b]=[d] \Rightarrow b \equiv d \pmod{n} \Rightarrow \exists\, k_2 \in \mathbb{Z} \ni b \equiv d+k_2 n.$

$a+b=(c+k_1 n)+(d+k_2 n) = c+d+n(k_1+k_2)$

$\Rightarrow (a+b) \equiv (c+d) \pmod{n}$

$\therefore [a+b]=[c+d].$

$ab = (c+k_1 n)(d+k_2 n) = cd + n(k_2 c + k_1 d + n k_1 k_2)$

$\Rightarrow ab \equiv cd \pmod{n}$

$\therefore [ab]=[cd].$ $\square$

EX: WRITE ADDITION AND MULTIPLICATION TABLES FOR $\mathbb{Z}_3$.

$+$	$[0]$	$[1]$	$[2]$
$[0]$			
$[1]$			
$[2]$			

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$			
$[1]$			
$[2]$			

PROPERTIES OF $\mathbb{Z}_n$

1) $+$ AND $\cdot$ ARE CLOSED (BINARY) OPERATORS.
2) $+$ AND $\cdot$ ARE COMMUTATIVE.
3) $+$ AND $\cdot$ ARE ASSOCIATIVE.
4) $\cdot$ IS DISTRIBUTIVE OVER $+$.
5) IDENTITIES ARE $[0]$ UNDER $+$, $[1]$ UNDER $\cdot$.
6) THE ADDITIVE INVERSE OF $[x]$ IS $[n-x]$.
7) MULTIPLICATIVE INVERSES EXIST ONLY FOR $x \ni \gcd(x,n)=1$.

THM: IF a AND n ARE COPRIME, THEN THERE EXISTS $b \in \mathbb{Z}$ SUCH THAT $ab \equiv 1 \pmod{n}$. WE CALL b THE MULTIPLICATIVE INVERSE OF a MODULO n. b IS UNIQUE MODULO n. WE WRITE

$$b = a^{-1} \pmod{n}.$$

PROOF: CONSIDER THE SET $\{0, a, 2a, 3a, \dots, (n-1)a\}$. IF WE CAN SHOW THAT THESE ARE ALL DISTINCT MODULO n, THEN EXACTLY ONE OF THEM IS EQUAL TO $1 \pmod{n}$.

SUPPOSE THE CONTRARY: $\exists\, c, d \in \mathbb{N} \cup \{0\}$, $c, d < n \ni ca \equiv da \pmod{n}$, $c \neq d$

THEN $(c-d)a \equiv 0 \pmod{n}$, SO $\exists k \in \mathbb{Z} \ni (c-d)a = kn$. BUT a AND n ARE COPRIME, SO $n \mid (c-d)$. THIS IS A CONTRADICTION, SINCE c AND d ARE DISTINCT NONNEGATIVE INTEGERS LESS THAN n. $\square$

EX: FIND A MULTIPLICATIVE INVERSE OF 43 MODULO 60.

A: WE NEED $x \in \mathbb{N}$ SUCH THAT $43x \equiv 1 \pmod{60}$. NOTICE THAT $43x$ MUST HAVE LAST DIGIT 1, SINCE 60 IS A MULTIPLE OF 10. SO ANY x SUCH THAT $43x$ ENDS IN 1 HAS LAST DIGIT 7. THE POSSIBILITIES ARE 7, 17, 27, 37, 47, 57.

$$43 \cdot 7 = 301 \equiv 1 \pmod{60}.$$

$$\therefore 43^{-1} = 7 \pmod{60}.$$

EX: FIND $3^{-1} \pmod{40}$.

A: BY THE SAME REASONING AS ABOVE, THE POSSIBILITIES ARE 7, 17, 27, 37.

$$3 \cdot 7 = 21 \equiv 21 \pmod{40}$$
$$3 \cdot 17 = 51 \equiv 11 \pmod{40}$$
$$3 \cdot 27 = 81 \equiv 1 \pmod{40}$$

$$\therefore 3^{-1} = 27 \pmod{40}.$$

APPLICATION : CRYPTOGRAPHY

CRYPTOGRAPHY IS THE STUDY OF METHODS FOR SENDING SECRET MESSAGES. THERE ARE MANY TECHNIQUES FOR ENCRYPTION AND DECRYPTION, ONE OF WHICH IS PUBLIC-KEY CRYPTOGRAPHY. THE METHOD USES BIG PRIME NUMBERS AND MODULAR ARITHMETIC. RSA IS ONE SUCH PUBLIC-KEY METHOD.

RSA

1) CHOOSE 2 LARGE PRIMES p, q.
2) CHOOSE $e \in \mathbb{Z}$ THAT IS COPRIME WITH $(p-1)(q-1)$.
3) CHOOSE $d \in \mathbb{Z} \ni ed \equiv 1 \pmod{(p-1)(q-1)}$.
4) THE PUBLIC KEY IS (e, pq). THIS IS AVAILABLE TO EVERYONE FOR ENCRYPTION.
5) THE PRIVATE KEY IS (d, pq). THIS IS AVAILABLE ONLY TO THOSE WHO THE SENDER WANTS TO BE ABLE TO DECRYPT.

ENCRYPTION STEP: LET THE MESSAGE TO BE ENCRYPTED BE $M \in \mathbb{Z}$, $0 \leq M < pq$ (A COMPUTER USES BINARY CODE FOR EVERYTHING, SO ENCRYPTING INTEGERS IS SUFFICIENT). THE ENCRYPTED MESSAGE IS $C = M^e \pmod{pq}$.

DECRYPTION STEP: M IS RECOVERED BY

$$M = C^d \pmod{pq}.$$

WE WILL NOT SEE THE PROOF. p AND q ARE CHOSEN TO BE SEVERAL HUNDRED DIGITS LONG EACH, MAKING IT IMPOSSIBLE FOR A COMPUTER TO FIND THE FACTORS $(p-1)(q-1)$ IN REASONABLE TIME. WE WILL SEE SOME EXAMPLES WITH SMALL PRIMES.

<u>EX</u>: LET $A=1, B=2, \dots, Z=26$, PUBLIC KEY $(3,55)$. ENCRYPT AND DECRYPT THE MESSAGE "HEY".

A: $pq=55 \Rightarrow p=5, q=11$. $e=3$, WHICH IS COPRIME WITH $(5-1)(11-1)=40$. THE UNENCRYPTED MESSAGE IS $8 \; 5 \; 25$.

$$8^3 = 64\cdot 8 \equiv 9\cdot 8 \pmod{55} = 72 \pmod{55} \equiv 17 \pmod{55}$$

$$5^3 = 125 \equiv 15 \pmod{55}$$

$$25^3 = 125\cdot 125 \equiv 15\cdot 15 \pmod{55} = 225 \pmod{55} \equiv 5 \pmod{55}.$$

THE ENCRYPTED MESSAGE IS $17 \; 15 \; 5$.

FROM A PREVIOUS EXAMPLE, $3^{-1} \pmod{40} = 27$.

$$17^{27} = 289^{13}\cdot 17 \equiv 14^{13}\cdot 17 \pmod{55} = 196^{6}\cdot 14\cdot 17 \pmod{55} = 196^{6}\cdot 238 \pmod{55}$$

$$\equiv 31^{6}\cdot 18 \pmod{55} = 961^{3}\cdot 18 \pmod{55} \equiv 26^{3}\cdot 18 \pmod{55}$$

$$= 676\cdot 468 \pmod{55} \equiv 16\cdot 28 \pmod{55} = 448 \pmod{55} \equiv 8 \pmod{55}$$

SO THE DECRYPTED 17 IS 8, THE ORIGINAL "H".

SIMILARLY, 15 DECRYPTED IS 5, AND 5 DECRYPTED IS 25.

<u>EXERCISE</u>: DECRYPT THE MESSAGE 41 83 36 THAT WAS ENCRYPTED WITH PUBLIC KEY $(5,91)$.

SET THEORY

A "SET" IS A LOOSELY-DEFINED COLLECTION OF ITEMS CALLED "ELEMENTS". SETS ARE COMPLETELY DETERMINED BY THEIR ELEMENTS, i.e. TWO SETS WITH EXACTLY THE SAME ELEMENTS ARE THE SAME SET. THE ORDER IN WHICH ELEMENTS ARE LISTED IS IRRELEVANT, AND ELEMENTS MAY BE LISTED MORE THAN ONCE WITHOUT CHANGING THE SET.

$$\{1,3\} = \{3,1\} = \{3,3,1,3,1,1\}.$$

THE COLLECTION OF ALL PEOPLE IN THIS ROOM IS A SET.

THE COLLECTION OF YOUR FAVOURITE SONGS IS A SET.

THE COLLECTION OF ALL REAL NUMBERS $\mathbb{R}$ IS A SET.

SETS COME FROM A <u>UNIVERSE</u> OF ELEMENTS $\mathcal{U}$. FOR EXAMPLE, THE SET OF EVEN NUMBERS COMES FROM THE UNIVERSE $\mathbb{Z}$. SETS CAN BE CONTAINED IN OTHER SETS, AND CAN BE FINITE OR INFINITE.

$$\{1,2,3\};\ \{\text{SUSAN, ROBERT}\};\ \{0,\{0\},1,\{0,1\}\};$$

$$\{2,4,6,\dots\};\ \{2,4,6,\dots,30\}.$$

SOME IMPORTANT SETS OF NUMBERS ARE

$\mathbb{N} = \{1,2,3,\dots\}$ (NATURAL)

$\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ (INTEGER)

$\mathbb{Q} = \{\frac{a}{b} : a,b \in \mathbb{Z}, b \neq 0\}$ (RATIONAL)

$\mathbb{R}$ = SET OF ALL REAL NUMBERS. (RATIONAL AND IRRATIONAL)

A SET CAN BE DEFINED BY A PROPERTY OF ELEMENTS OF A BIGGER SET. GIVEN A SET S, DEFINE A SET T BY

$$T = \{x \in S : p(x)\},$$ ALL THE ELEMENTS OF S THAT SATISFY p.

EX: THE SET $\{x \in \mathbb{R} : -2 < x \leq 5\}$ IS THE SET OF ALL REAL NUMBERS BETWEEN -2 AND 5, NOT INCLUDING -2. THIS SET IS AN INTERVAL, WHICH CAN BE DENOTED AS $(-2, 5]$.

EX: THE SET $\{x \in \mathbb{Z} : -2 < x \leq 5\}$ CAN BE REWRITTEN HOW?

EX: THE SET $\{x \in \mathbb{R} : x^3 = x\}$ CAN BE REWRITTEN HOW?

THE EMPTY SET IS THE SET WITH NO ELEMENTS, DENOTED BY $\emptyset$. IT CAN BE REPRESENTED IN DIFFERENT WAYS:

$$\{x \in \mathbb{N} : x \neq x\}; \quad \{x \in \mathbb{R} : 3 < x < 2\}.$$

A SET IS FINITE IF $\exists n \in \mathbb{N}$ SUCH THAT THERE IS A ONE-TO-ONE CORRESPONDENCE WITH THE SET $\{1, 2, \ldots, n\}$. FOR A SET S OF THIS SIZE, WE WRITE $|S| = n$ AND SAY THAT S HAS CARDINALITY n. NOTE: $|\emptyset| = 0$.

A SET THAT IS NOT FINITE IS SAID TO BE INFINITE.

SUBSETS

DEF: LET A AND B BE SETS. WE SAY A IS A SUBSET OF B, WRITTEN $A \subseteq B$, IFF EVERY ELEMENT OF A IS ALSO AN ELEMENT OF B.

SYMBOLICALLY,

$$A \subseteq B \iff \forall x, x \in A \Rightarrow x \in B.$$