Ch 0: # 3, 4, 10, 17, 21, 28, 37, 50, 58-60

3) $51 \bmod 13 = (13(3) + 12) \bmod 13 = 12$

$342 \bmod 85 = (85(4) + 2) \bmod 85 = 2$

$62 \bmod 15 = (15(4) + 2) \bmod 15 = 2$

$10 \bmod 15 = 10$

$82 \cdot 73 \bmod 7 = (7(11)+5)(7(10)+3) \bmod 7 = 5 \cdot 3 \bmod 7 = 15 \bmod 7 = 1$

$(51 + 68) \bmod 7 = ((7 \cdot 7 + 2) + (7 \cdot 9 + 5)) \bmod 7 = 2 + 5 \bmod 7 = 7 \bmod 7 = 0$

$(35 \cdot 24) \bmod 11 = (2 \cdot 24) \bmod 11 = (2 \cdot 2) \bmod 11 = 4$

$(47 + 68) \bmod 11 = (3 + 2) \bmod 11 = 5$

4) Find $s, t \in \mathbb{Z}$ s.t. $1 = 7s + 11t$

- $s = -3$ and $t = 2$ then $7s + 11t = -21 + 22 = 1$ ✓
- This is not unique. Take for ex, $s = -14$ and $t = 9$; again you get 1.

  In fact take $s = -3 - 11k$ and $t = 2 + 7k$, $k \in \mathbb{Z}_{\neq 0}$. Then you get 1

10) Let $a, b \in \mathbb{Z}_{>0}$, $d = \gcd(a,b)$, $m = \operatorname{lcm}(a,b)$.

- If $t \mid a$ and $t \mid b$, prove $t \mid d$.

  Since d is the $\gcd(a,b)$, $\exists\, u, v \in \mathbb{Z}$ s.t. $d = au + bv$. Since $t \mid a$, $a = k_1 t$ for some $k_1 \in \mathbb{Z}$. Similarly, $b = k_2 t$, $k_2 \in \mathbb{Z}$. So $d = k_1 t u + k_2 t v = t(k_1 u + k_2 v)$. Thus $t \mid d$.

- If s is a multiple of a and of b, prove s is a multiple of m.

  Using the division algorithm, $s = qm + r$ for some $r, q \in \mathbb{Z}$, $0 \le r < m$.
  Now $a \mid s$, $a \mid m$, $b \mid s$ and $b \mid m$. Thus $a \mid s - qm$ and $b \mid s - qm$.
  Hence, $a \mid r$ and $b \mid r$. but m is the $\operatorname{lcm}(a,b)$ and $r < m$. So r must be zero. $\therefore$ $s = qm$, or s is a multiple of m

37) $8 \times 8 \times 8 = 4 \mod n$ for what n?

$\Rightarrow 512 \mod n = 4$ for what n?

$\Rightarrow n \mid 512 - 4$

$\Rightarrow n \mid 508$

$\Rightarrow \boxed{n = 2, 4, 127, 254, \text{ or } 508}$

508 / 2, 254

254 / 2, 127

50) 0716? 28419 ISBN, Find ?

(From 49, $\cdot(10, 9, \ldots, 3, 2, 1) \mod 11$ should be 0.)

$(0, 7, 1, 6, x, 2, 8, 4, 1, 9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \mod 11$

$= 0 + 63 + 8 + 42 + 6x + 10 + 32 + 12 + 2 + 9 \mod 11$

$= 8 + 8 + 9 + 6x + 10 + \underbrace{10 + 1}_{11} + \underbrace{2 + 9}_{11} \mod 11$

$= 25 + 10 + 6x \mod 11$

$= 35 + 6x \mod 11$

$= 2 + 6x \mod 11$, and this must be 0.

$x = \cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, \cancel{9}$

$\Rightarrow \boxed{x = 7}$

58) $S = \mathbb{R}$, $a \sim b$ if $a - b \in \mathbb{Z}$

- Show $\sim$ is an equiv rltn.

reflexive: $a - a = 0 \in \mathbb{Z} \Rightarrow a \sim a$

symmetric: $a \sim b \Rightarrow a - b \in \mathbb{Z} \Rightarrow -(a-b) \in \mathbb{Z} \Rightarrow b - a \in \mathbb{Z} \Rightarrow b \sim a$

transitive: $a \sim b$, $b \sim c \Rightarrow a - b, b - c \in \mathbb{Z} \Rightarrow a - b + b - c \in \mathbb{Z} \Rightarrow a - c \in \mathbb{Z} \Rightarrow a \sim c$

- Equivalence classes: sets of real numbers with the same decimal part

(i.e. $a - [\![a]\!] = b - [\![b]\!] \Leftrightarrow a$ and b are in the same equiv. class)

alt, $[a] = \{a + k \mid k \in \mathbb{Z}\}$.

So the set of classes are $\{a \mid 0 \leq a < 1\}$

17) Let $a, b, s, t \in \mathbb{Z}$.

- If $a \bmod st = b \bmod st$, show $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$.

$$a \bmod st = b \bmod st \Rightarrow st \mid (a-b)$$
$$\Rightarrow s \mid (a-b) \quad \text{and} \quad t \mid (a-b)$$
$$\Rightarrow a \bmod s = b \bmod s \quad \text{and} \quad a \bmod t = b \bmod t$$

- What conditions on s and t make the converse true?

s and t relatively prime

21) Prove that there are infinitely many primes.

Suppose not. Then there is a finite set of primes, say $\{p_1, p_2, \dots, p_n\}$. Consider $q = p_1 p_2 \cdots p_n + 1$. None of the p_i divide q. So q must be prime, which is a contradiction.

28) Prove $2^n 3^{2n} - 1$ is always divisible by 17. $(n \in \mathbb{Z}_{\geq 0})$

Case 1: $n = 0$

$2^0 3^0 - 1 = 1 - 1 = 0$ and $17 \mid 0$.

Case 2: $n > 0$

If $n = 1$, $2 \cdot 3^2 - 1 = 17$ so $17 \mid 17$. Assume $17 \mid 2^n 3^{2n} - 1$.

Consider $2^{n+1} 3^{2(n+1)} - 1$:

$$2^{n+1} 3^{2(n+1)} - 1 = 2^n \cdot 2 \cdot 3^{2n} \cdot 3^2 - 1$$
$$= (2^n 3^{2n})(2 \cdot 3^2) - 1$$

Now, $17 \mid 2^n 3^{2n} - 1 \Rightarrow 2^n 3^{2n} - 1 = 17k$ for $k \in \mathbb{Z}$
$$\Rightarrow 17k + 1 = 2^n 3^{2n}.$$

So, subbing in, $2^{n+1} 3^{2(n+1)} - 1 = (17k+1)(2 \cdot 3^2) - 1$
$$= 17k(2 \cdot 3^2) + 2 \cdot 3^2 - 1$$
$$= 17k(2 \cdot 3^2) + 17$$
$$= 17(k(2 \cdot 3^2) + 1)$$

So $17 \mid 2^{n+1} 3^{2(n+1)} - 1$.

Note: You could do this by using that $2^{n+1} 3^{2(n+1)} - 1 = 18 \, 2^n 3^{2n} - 1$
$$= 18(2^n 3^{2n} - 1) + 17$$
$$= 18(17k) + 17$$
$$= 17(18k + 1).$$

59) $S = \mathbb{Z}$, aRb if $ab \geq 0$

This is not. an equivalence relation. It is not transitive.

for ex: $a = 1$, $b = 0$, $c = -1$

aRb since $+1 \cdot 0 = 0 \geq 0$ ✓

bRc since $0 \cdot -1 = 0 \geq 0$ ✓

but aRc is not true since $1 \cdot -1 = -1 \not\geq 0$.

60) $S = \mathbb{Z}$, aRb if $a+b$ is even.

- Show is equiv rltn.

reflevive: $a + a = 2a$, which is even

Symmetric: $aRb \Rightarrow 2 \mid (a+b) \Rightarrow 2 \mid (b+a) \Rightarrow bRa$

transitive: aRb and $bRc \Rightarrow a+b = 2k_1$ and $b+c = 2k_2 \Rightarrow a+c = a+2b+c-2b$

$$= (a+b)+(b+c)-2b$$

$$= 2k_1 + 2k_2 + 2(-b)$$

$$\Rightarrow 2 \mid a+c \Rightarrow aRc$$

- The equivalence class of an even number is all evens and of an odd is all odds.