1) $n=5$: $1, 2, 3, 4$

$n=8$: $1, 3, 5, 7$

$n=12$: $1, 5, 7, 11$

$n=25$: $1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19,$
$21, 22, 23, 24$

$n=20$: $1, 3, 7, 9, 11, 13, 17, 19$

3) $51 \bmod 13 = 12$

$342 \bmod 85 = 2$

$62 \bmod 15 = 2$

$10 \bmod 15 = 10$

$(82 \cdot 73) \bmod 7 = 5986 \bmod 7$
$= 1$

$(51+68) \bmod 7 = 0$

$(35 \cdot 24) \bmod 11 = 1320 \bmod 11 = 4$

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

5) male : $40(M-1)+b$

female : $40(M-1)+b+500$

m = birth month
b = birth date

42218 53953

$218 = 40(m-1)+b$ $953 = 40(m-1)+b+500$

$= 40m - 40 + b$ $453 = 40m - 40 + b$

$258 = 40m + b$ $493 = 40m + b$

$m = 6, \; b = 18$ $m = 12, \; b = 13$

18/6/1942 // 13/12/1953 //

7) Show $a, b \in \mathbb{Z}^{+} \Rightarrow ab = \text{lcm}(a,b) \cdot \gcd(a,b)$

$\gcd(a,b) = as + bt$

By Thm 0.3,

$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$

$b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$

$p_i \neq p_j, \; i \neq j$

$m_i, n_i \geq 0$

$\text{lcm}(a,b) = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}, \quad s_i = \max(m_i, n_i)$

$\gcd(a,b) = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, $t_i = \min(m_i, n_i)$

$\therefore \operatorname{lcm}(a,b)\gcd(a,b)$

$= p_1^{m_1+n_1} p_2^{m_2+n_2} \cdots p_k^{m_k+n_k}$

$= ab$

8) $a \mid c$, $b \mid c$

$\gcd(a,b) = 1 \Rightarrow ab \mid c$

$c = am = bn$

$1 = as + bt$

$c = c(as + bt)$

$= acs + bct$

$= a(bn)s + b(am)t$

$= ab(ns + mt)$

$\therefore ab \mid c$ //

Let $a = 6$, $b = 4$, $c = 12$, then

$\gcd(6,4) = 2$, $6 \mid 12$, $4 \mid 12$, but $6 \cdot 4 \nmid 12$ //

9) $a, b \in \mathbb{Z},\ n \in \mathbb{Z}^+$

WTS $a \bmod n = b \bmod n \iff n \mid a-b$

($\Rightarrow$) Let $a \bmod n = b \bmod n$

$$a = q_1 n + r_1$$
$$b = q_2 n + r_2$$

$$\therefore a - q_1 n = b - q_2 n$$
$$a - b = q_1 n - q_2 n$$
$$= (q_1 - q_2) n$$

$\therefore n \mid a-b$

($\Leftarrow$) Let $n \mid a-b$,

$$a-b = nk$$
$$a = q_1 n + r_1$$
$$b = q_2 n + r_2$$

$$a - b = q_1 n + r_1 - q_2 n - r_2$$
$$= (q_1 - q_2) n + r_1 - r_2$$

$\therefore r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

$\therefore a \bmod n = b \bmod n$ //

ii) $n \in \mathbb{Z}^+, n > 1$

$a \bmod n = a'$

$b \bmod n = b'$

WTS $(a+b) \bmod n = (a'+b') \bmod n$

$(ab) \bmod n = (a'b') \bmod n$

$$a = q_1 n + a'$$
$$b = q_2 n + b'$$

$$a+b = (q_1 + q_2) n + (a'+b')$$
$$(q_1 + q_2) n = (a+b) - (a'+b')$$

$\therefore\ n \mid (a+b) - (a'+b')$

By exercise 9,

$a \bmod n = b \bmod n \iff n \mid a-b$

$\therefore\ (a+b) \bmod n = (a'+b') \bmod n$ //

$$ab = (q_1 n + a')(q_2 n + b')$$

$$= q_1 q_2 n^2 + q_1 n b' + q_2 n a' + a'b'$$

$$= n(q_1 q_2 n + q_1 b' + q_2 a') + a'b'$$

$\therefore\ n \mid (ab) - (a'b')$

$\therefore\ ab \bmod n = a'b' \bmod n$ //

13) $n, a \in \mathbb{Z}^+$,

$d = \gcd(a, n)$

WTS $ax \bmod n = 1$ has a solution

iff $d=1$

$(\Rightarrow)$ Let $ax \bmod n = 1$ has a solution s

$$as = nq + 1$$

$$as - nq = 1$$

$$as + n(-q) = 1$$

$$d = \gcd(a,n) = as + n(-q) = 1$$

$(\Leftarrow)$ Let $d=1$

$$d = \gcd(a,n) = 1$$

$$\gcd(a,n) = as + nt = 1$$

$$as = -nt + 1$$

$$= n(-t) + 1$$

$$\therefore as \bmod n = 1 \;//$$

14) WTS $\forall n \in \mathbb{Z}$, $5n+3$ and $7n+4$ are relatively prime

Let $n=1$,

$5(1)+3=8$, $7(1)+4=11$

$$8(-4)+11(3) = -32+33$$
$$=1$$
$$=\gcd(8,11)$$

$\therefore \gcd(8,11)=1$

Let $n=k$,

$(5k+3)s+(7k+4)t=1$

$\therefore \gcd(5k+3,7k+4)=1$

Let $n=k+1$,

$[5(k+1)+3]s+[7(k+1)+4]t$

$= 5(\ldots - 3)s \ldots t \ldots - 1)t$

$= (5k+3)s + 5s + (7k+4)t + 7t$

$= 5s + 7t$

$= \gcd(5, 7)$

$= 1$

$\therefore \gcd(5(k+1)+3,\ 7(k+1)+4) = 1$

$\therefore$ By induction, $\forall n \in \mathbb{Z}$, $\gcd(5n+3, 7n+4) = 1$ //

18) $8^{402} \bmod 5$

$8^1 = 8,\ 8^2 = 64,\ 8^3 = 512,\ 8^4 = 4096,$
$8^5 = 32768, \ldots$

The last digit of 8^n is $8, 4, 2, 6$.

$402 \bmod 4 = 2$

$\therefore 8^{402} \bmod 5 = 4 \bmod 5 = 4$ //

20) $P_1, P_2, \ldots, P_n$ are primes, WTS

$P_1 P_2 \cdots P_n + 1$ is divisible by none of these primes.

$\because p \mid a+b \Leftrightarrow p \mid a \land p \mid b$

Since $n \mid 1 \Rightarrow n = 1$, and

$P_1, P_2, \ldots, P_n \neq 1$,

$\therefore P_i \nmid P_1 P_2 \cdots P_n + 1$ //

21) Let $P_1, P_2, \ldots, P_k$ be all prime numbers,

$\because \forall n \in \mathbb{N}, n > 1$,

n is prime $\lor$ n is a product of prime

$\therefore P_i \mid n$

Let $a = P_1 P_2 \cdots P_k$,

$a \in \mathbb{N} \Rightarrow a+1 \in \mathbb{N}$

$\therefore$ $a+1$ is a prime $\vee$ $P_i \mid a+1$

$\because$ $P_i \nmid P_1 P_2 \cdots P_k + 1$

$\therefore$ $a+1$ is a prime $(\Rightarrow\Leftarrow)$

$\therefore$ There are infinite number of primes. //

30) $f_1 = 1,\ f_2 = 1,\ f_n = f_{n-1} + f_{n-2},\ n \geq 3$

WTS $f_n < 2^n$

Let $n = 1$, $f_1 = 1 < 2^1 = 2$

Let $n = k$, $f_k = f_{k-1} + f_{k-2} < 2^k$

Let $n = k+1$,

$f_{k+1} = f_{k+1-1} + f_{k+1-2}$

$= f_k + f_{k-1}$

$< 2^k + 2^k = 2 \cdot 2^k$

$= 2^{k+1}$

$\therefore f_n < 2^n$ //

$\gcd(7563, 526)$

$7563 = 526(14) + 199$

$526 = 199(2) + 128$

$199 = 128(1) + 71$

$128 = 71(1) + 57$

$71 = 57(1) + 14$

$57 = 14(4) + 1$

$14 = 1(14) + 0$

52) $S \subseteq \mathbb{R}$, $a, b \in S$

$a \sim b$ if $a - b \in \mathbb{Z}$

i) $a - a = 0 \in \mathbb{Z} \Rightarrow a \sim a$

ii) let $a - b \in \mathbb{Z} \Rightarrow a \sim b$

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

$\therefore a \sim b \Rightarrow b \sim a$

iii) let $a - b \in \mathbb{Z}$, $b - c \in \mathbb{Z}$

$a - c = a - b + b - c$

$= (a-b) + (b-c) \in \mathbb{Z}$

$\therefore a \sim b,\ b \sim c \Rightarrow a \sim c$

53) $S \subseteq \mathbb{Z}$, $a, b \in S$,

aRb if $ab \geq 0$

i) $aa \geq 0 \Rightarrow a \sim a$

ii) $ab \geq 0 \Rightarrow ba \geq 0$

$\therefore aRb \Rightarrow bRa$

iii) $(1,0) \in R$, $(0,-1) \in R$

$(1,-1) \notin R$

No//