1. $19 = 7 \cdot 2 + 5$ ← remainder

↑ quotient

$-111 = 11 \cdot (-11) + 10$

$789 = 23 \cdot 34 + 7$

$0 = 9 \cdot 0 + 9$

$1001 = 77 \cdot 13 + 0$

$3 = 5 \cdot 0 + 3$

$-1 = 3 \cdot (-1) + 2$

$4 = 1 \cdot 4 + 0$

2. $X \equiv a \pmod{m}$

$$\bmod\left(\frac{X}{m}\right) = \bmod\left(\frac{a}{m}\right)$$

$X = at + m$

$$f(x) = \begin{cases} x \bmod m & \text{if } x \bmod m \le [m/2] \\ (x \bmod m) - m & \text{if } x \bmod m > [m/2] \end{cases}$$

3. $ac \equiv bc \pmod{m}$ $\quad m = 4 \quad ac = 0$

$a \not\equiv b \pmod{m}$ $\quad c = 2 \quad bc = 4$

$a = 0$

$b = 2$

$a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$ $\Rightarrow$ $a^c \not\equiv b^d \pmod{m}$

$m = 5$

$a = 3$

$b = 3$

$c = 1$

$d = 6$

$a^c = 3 \pmod{5}$

$b^d = 729 \equiv 4 \pmod{5}$

$3^1 \not\equiv 3^6 \pmod{5}$

$3 \equiv 3 \pmod{5}$

$1 \equiv 6 \pmod{5}$

4. a, b, k, m $k \geq 1$, $m \geq 2$, $a \equiv b \pmod{m}$

$a^k \equiv b^k \pmod{m}$

$a \cdot a \equiv b \cdot b \pmod{m}$ $\Rightarrow$ $a^2 \equiv b^2 \pmod{m}$

$a^3 \equiv b^3 \pmod{m}$

and after $k-1$ applications

$a^k \equiv b^k \pmod{m}$

5. $\mathbb{Z}_5$ for $+_m$ and $\cdot_m$

$+_m$ — $a +_m b = (a+b) \pmod{m}$

$\cdot_m$ — $a \cdot_m b = (ab) \pmod{m}$

$0+0=0$	$0+1=1$	$0+2=2$	$0+3=3$	$0+4=4$
$1+0=1$	$1+1=2$	$1+2=3$	$1+3=4$	$1+4=0$
$2+0=2$	$2+1=3$	$2+2=4$	$2+3=0$	$2+4=1$

$3+0=3$ $\quad 3+1=4$ $\quad 3+2=0$ $\quad 3+3=1$ $\quad 3+4=2$

$4+0=4$ $\quad 4+1=0$ $\quad 4+2=1$ $\quad 4+3=2$ $\quad 4+4=3$

$0\cdot 0=0$ $\quad 0\cdot 1=0$ $\quad 0\cdot 2=0$ $\quad 0\cdot 3=0$ $\quad 0\cdot 4=0$

$1\cdot 0=0$ $\quad 1\cdot 1=1$ $\quad 1\cdot 2=2$ $\quad 1\cdot 3=3$ $\quad 1\cdot 4=4$

$2\cdot 0=0$ $\quad 2\cdot 1=2$ $\quad 2\cdot 2=4$ $\quad 2\cdot 3=1$ $\quad 2\cdot 4=3$

$3\cdot 0=0$ $\quad 3\cdot 1=3$ $\quad 3\cdot 2=1$ $\quad 3\cdot 3=4$ $\quad 3\cdot 4=2$

$4\cdot 0=0$ $\quad 4\cdot 1=4$ $\quad 4\cdot 2=3$ $\quad 4\cdot 3=2$ $\quad 4\cdot 4=1$

6. $f(a)= a \text{ div } d$ $\qquad d=3 \qquad a=3,6,9 \qquad 0$

$g(a)= a \bmod d$

if $d=1$

one-to-one, onto

neither

7.

231 | 2
−230 → 1 | 115 | 2
−114 → 1 | 57 | 2
−56 → 1 | 28 | 2
−28 → 0 | 14 | 2
0 | 7 | 2
−6 → 1 | 3 | 2
1 | 1 | 2
−1 → 1 | 0

11100111

$4532 = (1000110110100)_2$

$97644 = (10111110101101100)_2$

8. $(11111)_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 =$

$= 1 + 2 + 4 + 8 + 16 = 31$

$(10\ 0000\ 0001)_2 = 1 \cdot 2^0 + 2^9 = 1 + 2^9 = 513$

$(1\ 0101\ 0101)_2 = 2^8 + 2^6 + 2^4 + 2^2 + 2^0 = 341$

$(110100100010000)_2 = 2^{14} + 2^{13} + 2^{11} + 2^8 + 2^4 = 26896$

9. $(1000111)_2 + (111\ 0111)_2 = 1011\ 1110$

$(1000111)_2 \cdot (111\ 0111)_2 = 10\ 0001\ 0000\ 0001$

$(1110\ 1111)_2 + (10111101)_2 = 1\ 1010\ 1100$

$(1110\ 1111)_2 \cdot (10111101)_2 = 1011\ 0000\ 0\ 1110011$

$10\ 1010\ 1010 + 111110000 = 10010011010$

$101010\ 1010 \cdot 111110000 = 101\ 0010\ 1001\ 0110\ 0000$

10. $88 = 2^3 \cdot 11$ $\quad 126 = 2 \cdot 3^2 \cdot 7$ $\quad 729 = 3^6$

$$\begin{array}{r|l} 88 & 2 \\ 44 & 2 \\ 22 & 2 \\ 11 & \end{array} \qquad \begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & \end{array} \qquad \begin{array}{r|l} 729 & 3 \\ 243 & 3 \\ 81 & 3 \\ 27 & 3 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}$$

$1001 = 7 \cdot 11 \cdot 13$

$$\begin{array}{r|l} 1001 & 7 \\ 143 & 11 \\ 13 & \end{array}$$

11\. 100! how many zeros are in the end?

$10 = 2 \cdot 5 \Rightarrow \text{Num} = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor + \dots$

$\quad 20 \quad 4 \quad \dots \quad = 24$

12\. $\gcd(12,18) = \gcd(12, 18 \bmod 12) =$

$= \gcd(12,6) = \gcd(6,0) = \boxed{6}$

$\gcd(111,201) = \gcd(111, 201 \bmod 111) =$

$= \gcd(111,90) = \gcd(90, 111 \bmod 90) =$

$= \gcd(90,21) = \gcd(21, 90 \bmod 21) =$

$= \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = \boxed{3}$

$\gcd(1001,1331) = \gcd(1001,330) = \gcd(330,11) =$

$= \gcd(11,0) = \boxed{11}$

$\gcd(12345, 54321) = \gcd(12345, 4941) = \gcd(4941,$

$2463) = \gcd(2463,15) = \gcd(15,3) = \gcd(3,0) = \boxed{3}$

$gcd(1000, 5040) = gcd(1000, 40) = gcd(40, 0) = \boxed{40}$

$gcd(9888, 6060) = gcd(6060, 3828) = gcd(3828, 2232) = gcd(2232, 1596) = gcd(1596, 636) =$

$= gcd(636, 324) = gcd(324, 312) = gcd(312, 12) =$

$= gcd(12, 0) = \boxed{12}$