Basics

Problem 1. $1+4+7+7+13+16+19+19+\cdots+991+991+997+1000 = \sum_{i=0}^{333} 1+3i - 83\times 3 = \frac{(1+1000)\times 334}{2} - 249 = 166918$

Problem 2.

$$\begin{aligned} 2101 &= 2\times 1009 + 83 \\ 1009 &= 12\times 83 + 13 \\ 83 &= 6\times 13 + 5 \\ 13 &= 2\times 5 + 3 \\ 5 &= 1\times 3 + 2 \\ 3 &= 1\times 2 + 1 \end{aligned}$$

So $\gcd(2101, 1009) = 1$

Problem 3. First find the GCD of 12345 and 211.

$$\begin{aligned} 12345 &= 58\times 211 + 107 \\ 211 &= 1\times 107 + 104 \\ 107 &= 1\times 104 + 3 \\ 104 &= 34\times 3 + 2 \\ 3 &= 1\times 2 + 1 \end{aligned}$$

By rewriting the expressions,

$$\begin{aligned} 12345 - 58\times 211 &= 107 \\ 211 - 1\times 107 &= 104 = 59\times 211 - 12345 \\ 107 - 1\times 104 &= 3 = 2\times 12345 - 117\times 211 \\ 104 - 34\times 3 &= 2 = 4037\times 211 - 69\times 12345 \\ 3 - 1\times 2 &= 1 = 71\times 12345 - 4154\times 211 \end{aligned}$$

Hence 12345^{-1} modulo 211 is 71.

Problem 4. Required answer is future value $= 1000\times 1.05^5 \approx \$1,276$

Problem 5. Required answer is current value $= \frac{100000}{1.10^{10}} \approx \$38,554$

Problem 6.

(a) $\gcd(19, 77) = 1$, therefore the inverse exists and 19^{-1} modulo 77 is 73.
Mutiplying 73 on both sides yeilds $x \equiv 20 \times 73 \equiv 74 \pmod{77}$

(b) $\gcd(49, 21) = 7$, we rewrite the given form as $7x \equiv 14 \pmod 3$.
7^{-1} modulo 3 is 1, therefore we have $x \equiv 2 \pmod 3$.

(c) Although $\gcd(105, 100) = 5$, $5 \not| 143$. Therefore unsolvable.

Medium

Problem 1.

$$\begin{aligned} 987 \bmod 17 &= 1 \\ 987^2 \bmod 17 &= 1 \\ 987^4 \bmod 17 &= 1 \\ &\vdots \\ 987^{64} \bmod 17 &= 1 \end{aligned}$$

And we have $987^{65} \bmod 17 = 1$.

Problem 2. Let $N = \sum_{i=0}^{k} 10^i d_i$, where k is the largest integer such that $10^k \leq N$. Since $10 \equiv 4 \pmod 6$, we have $100 \equiv 4 \pmod 6$. By repeating the process we will have $10^i \equiv 4 \pmod 6$ for any positive integer i. As $N \equiv \sum_{i=0}^{k} 10^i d_i \pmod 6$, it follows that $N \equiv \sum_{i=0}^{k} 4d_i = 4 \sum_{i=0}^{k} \pmod 6$. We can simply reduce it into $N \equiv 0 \pmod 2$ and $N \equiv \sum i = 0^k d_i \pmod 3$. The later shows that N should be divisible by 3 since $N \equiv \sum_{i=0}^{k} d_i \equiv \sum_{i=0}^{k} 10^i d_i \pmod 3$.

Problem 3. $f(100, 3) = \dfrac{100!}{3!97!} = \dfrac{100}{1} \times \dfrac{99}{2} \times \dfrac{98}{3}$. Hence $f(100, 3) \bmod 7 = (100 \times (99 \times 2^{-1}) \times (98 \times 3^{-1})) \bmod 7$. By using Fermat's little theorem or using extended Euclid's Algorithm, $2^{-1} = 4$ and $3^{-1} = 5$ modulo 7. The answer is $(100 \times 99 \times 98 \times 4 \times 5) \bmod 7 = (2 \times 1 \times 0 \times 4 \times 5) \bmod 7 = 0$.

Problem 4. Without loss of generality, assume $p \not| a$. Then by spc we know $rp + sa = 1$ for some integer r and s. Multiplying both sides by b, we have $(rb)p + s(ab) = b$. If $p|ab$, $p = kab$ for some integer k. Then we have $b = (rb)p + (sk)p$, which shows that b is a multiple of p and thus $p|b$.

Problem 5. By Fermat's little theorem, $x^4 \equiv 1 \pmod 5$. We have $x^{2110} \equiv x^{4 \times 527} \times x^2 \equiv x^2 \equiv 2 \pmod 5$. By trying $x = 1, 2, 3$, and 4, none of them gives 2 as remainder for $x^2 \bmod 5$. Therefore no solution.

Problem 6.

(a) $N = 31 \times 19 = 589$, $T = 30 \times 18 = 540$. By calculating $\gcd(101, 540)$

$$\begin{aligned} 540 &= 5 \times 101 + 35 \\ 101 &= 2 \times 35 + 31 \\ 35 &= 1 \times 31 + 4 \\ 31 &= 7 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \end{aligned}$$

So $\gcd(101, 540) = 1$ and therefore d exists. We find d by using extended Euclid's algorithm.

$$\begin{aligned} 540 - 5 \times 101 &= 35 \\ 101 - 2 \times 35 &= 31 = 11 \times 101 - 2 \times 540 \\ 35 - 1 \times 31 &= 4 = 3 \times 540 - 16 \times 101 \\ 31 - 7 \times 4 &= 3 = 123 \times 101 - 23 \times 540 \\ 4 - 1 \times 3 &= 1 = 26 \times 540 - 139 \times 101 \end{aligned}$$

Therefore $d = 540 - 139 = 401$.

(b)

$$\begin{aligned} 777 \bmod 589 &= 188 \\ 777^2 \bmod 589 &= 4 \\ 777^4 \bmod 589 &= 16 \\ 777^8 \bmod 589 &= 256 \\ 777^{16} \bmod 589 &= 157 \\ 777^{32} \bmod 589 &= 500 \\ 777^{64} \bmod 589 &= 264 \end{aligned}$$

So $777^{101} \bmod 589 = (777 \times 777^4 \times 777^{32} \times 777^{64}) \bmod 589 = (188 \times 16 \times 500 \times 264) \bmod 589 = 498$ and $m' \equiv 498 \pmod{589}$.

(c)

$$\begin{aligned}
498 \bmod 589 &= 498 \\
498^2 \bmod 589 &= 35 \\
498^4 \bmod 589 &= 47 \\
498^8 \bmod 589 &= 442 \\
498^{16} \bmod 589 &= 405 \\
498^{32} \bmod 589 &= 283 \\
498^{64} \bmod 589 &= 574 \\
498^{128} \bmod 589 &= 225 \\
498^{256} \bmod 589 &= 560
\end{aligned}$$

So $498^{401} \bmod 589 = (498 \times 498^{16} \times 498^{128} \times 498^{256}) \bmod 589 = (498 \times 405 \times 225 \times 560) \bmod 589 = 188$ and $m \equiv 188 \pmod{589}$.
Note: In practise N would be much greater than m and recovery of m is always possible.

Problem 7.

- **Step 1.** $N = 3 \times 5 \times 7 = 105$.
- **Step 2.** $N_1 = 35$, $N_2 = 21$, $N_3 = 15$.
- **Step 3.** $N_1^{-1} = 2$, $N_2^{-1} = 1$, $N_3 = 1$.
- **Step 4.** $x \equiv 2 \times 35 \times 2 + 1 \times 21 \times 1 + 4 \times 15 \times 1 \equiv 11 \pmod{105}$.
- **Step 5.** Since $x \geq 100$, smallest $x = 11 + 105 = 116$.

Problem 8.

(a) Suppose $n_i | x$ for $i = 1, 2, \cdots, k$ but $n_1 n_2 \cdots n_k \not| x$. There exists an index $1 \leq m < k$ such that $\prod_{i=1}^{m} n_i | x$ and $n_{m+1} \not| (\frac{x}{\prod_{i=1}^{m} n_i})$.
Let $p = \prod_{i=1}^{m} n_i$, we have $x = pq$ for some positive integer q.
Since $\gcd(a, c) \gcd(b, c) = 1 \implies \gcd(ab, c) = 1$, applying it repeatedly, we have $\gcd(p, n_{m+1}) = 1$.
Therefore, $n_{m+1} | x = pq$ implies $n_{m+1} | q = \frac{x}{p}$, which contradicts our assumption.

(b) Consider a solution y satisfying the given requirements. We have $y - x \equiv a_i - a_i \equiv 0 \pmod{n_i}$, and hence $n_i | y - x$ for $i = 1, 2, \cdots, k$.
With the fact that n_i's are pairwise coprime, we apply (a)(i) to get $n | y - x$.
Therefore $y - x \equiv 0 \pmod{n}$ and hence $y \equiv x \pmod{n}$.

Problem 9.

$$\begin{aligned} 342 &= 1 \times 243 + 99 \\ 243 &= 2 \times 99 + 45 \\ 99 &= 2 \times 45 + 9 \\ 45 &= 5 \times 9 + 0 \end{aligned}$$

So we have $\text{spc}(342, 243) = 9$. In addition,

$$\begin{aligned} 342 - 1 \times 243 &= 99 \\ 243 - 2 \times 99 &= 45 = 3 \times 243 - 2 \times 342 \\ 99 - 2 \times 45 &= 9 = 5 \times 342 - 7 \times 243 \end{aligned}$$

Therefore we have $99 = 55 \times 342 - 77 \times 243$.
We can fill the 342-gallon jug and pour the water into the 243-gallon jug for 55 times. Whenever the 243-gallon jug become full, empty it out. In the end, we will get 99 gallons of water.

To reduce number of rounds of transferring water, observe that $342 \times 27 - 243 \times 38 = 0$.
Then we have $342 \times 54 - 243 \times 76 = 0$. And we get $342 \times (55 - 54) - 243 \times (77 - 76) = 99$, which becomes $342 \times 1 - 243 \times 1 = 99$. We finally see that using 342-gallon jug once is enough.

Problem 10. $m^{13} - m = m(m^12 - 1)$. It is trivial to see that if m is a multiple of 13, $m(m^12 - 1)$ is divisible by 13.
If m is not a multiple of 13, $\gcd(m, 13) = 1$ since 13 is prime. By Fermat's little theorem, $m^12 \equiv 1 \pmod{13}$, which implies $m^12 - 1 \equiv 0 \pmod{13}$ and hence $m(m^12 - 1)$ is divisible by 13.

Problem 11.

(a) $22^{90} \bmod 91 = 1$, $22^{45} \bmod 91 = 1$. *Probably prime.*
$29^{90} \bmod 91 = 1$, $29^{45} \bmod 91 = 1$. *Probably prime.*
$38^{90} \bmod 91 = 1$, $38^{45} \bmod 91 = 90$. *Probably prime.*

(b) Choose 18 as base. As $18^{90} \bmod 91 = 64$, 91 is composite. In fact, $91 = 7 \times 13$.

Problem 12. Let x be the least number of eggs. The corresponding modulo equations are

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

Moving out redundant modulo equations, we get

$$\begin{aligned}x &\equiv 2 \pmod 3\\ x &\equiv 3 \pmod 4\\ x &\equiv 4 \pmod 5\\ x &\equiv 0 \pmod 7\end{aligned}$$

- **Step 1.** $N = 3 \times 4 \times 5 \times 7 = 420$.
- **Step 2.** $N_1 = 140$, $N_2 = 105$, $N_3 = 84$. We don't care about N_4 because $a_4 = 0$.
- **Step 3.** $N_1^{-1} = 2$, $N_2^{-1} = 1$, $N_3^{-1} = 4$. We don't care about N_4^{-1} because $a_4 = 0$.
- **Step 4.** $x \equiv 2 \times 140 \times 2 + 3 \times 105 \times 1 + 4 \times 84 \times 4 \equiv 119 \pmod{420}$
- **Step 5.** The given form in the previous step is smallest for x, therefore $x = 119$.

Problem 13.

(a) The antique is worth $2000000 \times 1.06^{20} \approx \$6,414,271$ after 20 years.

(b) Assume the payment is made at the end of each year. Let V be the loan, $\frac{1}{r} = b$ be the interest rate. Then annual payment is given by $\frac{V}{r} \times \frac{1-r}{1-r^{20}} \approx \$267,758$ By doing investment, his wealth can be considered by the total future value $= \sum_{i=0}^{19} 267,758 \times 1.12^i \approx \$19,292,618$.

Obviously, John should do investment instead of buying antique.

Problem 14. By rewriting $f(x, y, z)$, we have

$$\begin{aligned}f(x,y,z) &= 6 \times \frac{\frac{x}{y} + \frac{1}{2}\sqrt{\frac{y}{z}} + \frac{1}{2}\sqrt{\frac{y}{z}} + \frac{1}{3}\sqrt[3]{\frac{z}{x}} + \frac{1}{3}\sqrt[3]{\frac{z}{x}} + \frac{1}{2}\sqrt[3]{\frac{z}{x}}}{6}\\ &\geq 6 \times \sqrt[6]{\frac{x}{y} \cdot \frac{1}{2}\sqrt{\frac{y}{z}} \cdot \frac{1}{2}\sqrt{\frac{y}{z}} \cdot \frac{1}{3}\sqrt[3]{\frac{z}{x}} \cdot \frac{1}{3}\sqrt[3]{\frac{z}{x}} \cdot \frac{1}{3}\sqrt[3]{\frac{z}{x}}} \qquad \text{(By A.M. } \geq \text{ G.M.)}\\ &= 6 \times \sqrt[6]{\frac{1}{2 \times 2 \times 3 \times 3 \times 3} \frac{x}{y}\frac{y}{z}\frac{z}{x}}\\ &= 2^{\frac{2}{3}} \times 3^{\frac{1}{2}}\end{aligned}$$

Equality holds if and only if $\frac{x}{y} = \frac{1}{2}\sqrt{\frac{y}{z}} = \frac{1}{3}\sqrt[3]{\frac{z}{x}}$.