Introduction to Number Theory
3. exercise set, solutions

1. Let n be the number of soldiers in Han Xing's army. We know that n satisfies the following system of congruence equations

$$\begin{cases} n \equiv 5 \pmod 7 \\ n \equiv 9 \pmod{10} \\ n \equiv 9 \pmod{11} \end{cases}$$

Using the construction in the proof of the Chinese remainder theorem one easily finds that $5 \cdot 330 + 9 \cdot 231 + 9 \cdot 210 = 5619$ is a solution for the system. Thus the general solution is $n \equiv 5619 \pmod{770}$ or $n \equiv 229 \pmod{770}$. Thus the least possible number of soldiers in the army is 229.

2. (i) One easily checks that the units in $\mathbb{Z}_{12}$ are $[1]_{12} = [1]_{12}^{-1}$, $[5]_{12} = [5]_{12}^{-1}, [7]_{12} = [7]_{12}^{-1}$ and $[11]_{12} = [11]_{12}^{-1}$. The number of units is $4 = \varphi(12)$, as required.

(ii) Again one easily checks that the units in $\mathbb{Z}_{20}$ are $[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}$ and $[19]_{20}$. The inverses are $[1]_{20}, [7]_{20}, [3]_{20}, [9]_{20}, [11]_{20}, [17]_{20}, [13]_{20}$ and $[19]_{20}$, respectively. The number of units is $8 = \varphi(20)$, as required.

3. Let $n \in \mathbb{Z}_+$ be s.t. $\varphi(n) = 12$. Let p be a prime divisor of n. Then $p - 1|\varphi(n) = 12$ so $p \leq 13$. Note that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then

$$\varphi(n) = \varphi(P_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) \geq (p_1 - 1) \cdots (p_k - 1).$$

As $(2-1)(3-1)(5-1)(7-1) > 12$ it follows that n can have at most three prime factors. Now there are three different cases.

$1°$) Assume that n has exactly three prime factors. Then the must be $2, 3, 5$ or $2, 3, 7$ as $(2-1)(3-1)(11-1) > 12$. In the former case $(3-1)(5-1)|\varphi(n)$ which is not possible. So let $n = 2^\alpha 3^\beta 7^\gamma$. Then $12 = \varphi(n) = 2^{\alpha-1} 3^{\beta-1} 7^{\gamma-1} \cdot 2 \cdot 6 = 12 \cdot 2^{\alpha-1} 3^{\beta-1} 7^{\gamma-1}$ and thus $\alpha = \beta = \gamma = 1$. Hence $n = 2 \cdot 3 \cdot 7 = 42$ which indeed works.

$2°$) Assume that n has exactly two prime factors. Write $n = p^\alpha q^\beta$. Then $\varphi(n) = p^{\alpha-1} q^{\beta-1}(p-1)(q-1)$. Now there are four subcases:

2a) Assume that $\alpha = \beta = 1$. Then we have $(p-1)(q-1) = 12$. One easily checks that all the solutions are $(p, q) = (2, 13), (3, 7)$ and their permutations. This leads to solutions $n = 26$ and $n = 21$.

2b) Assume that $\alpha = 1$ and $\beta > 1$. Then we have $12 = \varphi(n) = q^{\beta-1}(p-1)(q-1)$. As $12 = 2 \cdot 2 \cdot 3$ it follows that $q = 2$ or $q = 3$. If $q = 2$, then it easy to see that $\beta \leq 3$. In the case $\beta = 2$ we have $p = 7$. In this case $n = 28$. If $\beta = 3$ there are no solutions. If $q = 3$, then it is easy to check that $\beta \leq 2$. If $\beta = 2$ one gets $p = 3$ which is not possible as $p \neq q = 3$.

2c) The case $\beta = 1$, $\alpha > 1$ is symmetric with the case 2b).

2d) Assume that $\alpha, \beta > 1$. In this case one of the prime factors must be 2 since otherwise $\varphi(n) > 3 \cdot 5 > 12$. Thus $2^{\alpha-1} q^{\beta-1}(q-1) = 12$. We clearly have $\alpha \leq 3$. If $\alpha = 2$ one easily gets $q = 3$ and $\beta = 2$. Thus $n = 4 \cdot 9 = 36$. If $\alpha = 3$ there are no solutions.

3°) Assume that n has exactly one prime factor. If $n = p^\alpha$ then $12 = \varphi(n) = p^{\alpha-1}(p-1)$ and it is straightforward to check that $p = 13, \alpha = 1$ is the only solution. Thus $n = 13$.

Therefore the complete set of solutions is $n = 13, 21, 26, 28, 36, 42$.

4. Write

$$f(x) \equiv \sum_{i=1}^{n} a_i x^i \pmod{m}.$$

Then, as $x^i - a^i = (x-a)(x^{i-1} + x^{i-2}a + \cdots + xa^{i-2} + a^{i-1})$, it follows that

$$\begin{aligned}
f(x) &\equiv \sum_{i=1}^{n} a_i x^i \\
&\equiv \sum_{i=1}^{n} a_i \left(a^i + (x-a)(x^{i-1} + x^{i-2}a + \cdots + xa^{i-2} + a^{i-1})\right) \\
&\equiv \sum_{i=1}^{n} a_i a^i + (x-a)\sum_{i=1}^{n} a_i(x^{i-1} + x^{i-2}a + \cdots + xa^{i-2} + a^{i-1}) \\
&\equiv f(a) + (x-a)g(x) \\
&\equiv (x-a)g(x) \pmod{m}.
\end{aligned}$$

Clearly deg $g = n - 1$, so the proof is completed. □

5. It is enough to show that if n is composite, then $2^n - 1$ is also composite. So, let $n = ab$ with $a, b \geq 2$. Now

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1),$$

which shows that $2^n - 1$ is composite. □

6. (i) If m is prime the claim follows immediately from Fermat's little theorem as $\varphi(m) = m - 1$ in this case. Suppose then m is a product of distinct primes; $m = p_1 \cdots p_k$. Then, as $\varphi(p_\ell) | \varphi(m)$, it follows that $2^{\varphi(p_\ell)} - 1 | 2^{\varphi(m)} - 1$. If $p_\ell \neq 2$ it follows that $p_\ell | 2^{\varphi(m)} - 1$ as by Fermat's little theorem $p_\ell | 2^{\varphi(p_\ell)} - 1$. If $p_\ell = 2$, then $p_\ell | 2$. Thus $p_1 \cdots p_k | 2(2^{\varphi(m)} - 1)$, as desired. □

b) No, take $m = 4$ and $a = 2$.

7. Let $p_1, p_2, ..., p_{k+1}$ be distinct primes. The problem is equivalent to that the system

$$\begin{cases} n \equiv 0 \pmod{p_1^2} \\ n \equiv -1 \pmod{p_2^3} \\ \vdots \\ n \equiv -(k-1) \pmod{p_k^{k+1}} \end{cases}$$

has a solution. But this follows directly from the Chinese remainder theorem as $(p_i^\ell, p_j^m) = 1$ for all $1 \leq i \neq j \leq k$ and $2 \leq \ell \neq m \leq k + 1$. □

8*. Assume that value of the polynomial $P(x)$ is integral for every integer x. We use induction on the degree n of the polynomial. If $n = 1$, then $P(x)$ is clearly of the required form. Assume that the statement is true for polynomial of degree $n-1$. Note that if deg $P = n$, then deg $Q = n-1$ where $Q(x) = P(x+1) - P(x)$. By induction hypothesis we can write

$$Q(x) = a_{n-1}\binom{x}{n-1} + \cdots + a_0\binom{x}{0}.$$

Observe that for every integer $x > 0$ we have $P(x) = P(0) + Q(0) + \cdots + Q(x)$. Then using the identity

$$\binom{0}{k} + \binom{1}{k} + \cdots + \binom{x-1}{k} = \binom{x}{k+1}$$

for every $x, k \in \mathbb{Z}_+$ we get the required representation

$$P(x) = a_{n-1}\binom{x}{n} + \cdots + a_0\binom{x}{1} + P(0).$$

The converse direction is obvious. This completes the proof. $\square$