Number Theory 1

zc231

1. (i) $205 \times 160 - 39 \times 841 = 1$. (ii) $65 \times 2171 - 54 \times 2613 = 13$.

2. (i) Take $b|a$, for example, $b = 1111, a = 9999$. (ii) Take two consecutive Fibonacci numbers, for example, $b = 1597$, $a = 2584$ where b is the 17th Fibonacci number and a is the 18th Fibonacci number so $\lambda(a, b) = 16$.

   (iii) We may assume that $(a, b) = 1$ because for any $d > 1$, $\lambda(a, b) = \lambda(ad, bd)$ (so for each step of finding the greatest common divisor of (a, b) we multiply both sides of the equation by d, then this is exactly the same as the algorithm to compute (ad, bd)). Now suppose we write $a = r_0, b = r_1$ and implement Euclidean algorithm,

   $$r_0 = q_1 r_1 + r_2, r_1 = q_2 r_2 + r_3, \cdots, r_{k-2} = q_{k-1} r_{k-1} + r_k, r_{k-1} = q_k r_k$$

   where $\lambda(a, b) = k$ and since $(a, b) = 1$ so $k \geq 2$ and $r_k = 1$. We may assume $q_1 = 1$ because the number of steps of computing (a', b) is also k where $a' = b + r_2$.

   As each $q_i \geq 1$ so using $r_i = q_{i+1} r_{i+1} + r_{i+2}$ we have $r_i \geq r_{i+1} + r_{i+2}$ and since $r_{i+1} > r_{i+2}$ we have $r_i > 2r_{i+2}$. Then by induction we see if k is even then $b > r_1 > 2^{\frac{k}{2}-1}$ (as $r_k = 1$) and if k is odd then $b = r_1 > 2^{\frac{k-1}{2}}$. So we have

   $$k < 2\frac{\log b}{\log 2} + 2 \text{ or } k < 2\frac{\log b}{\log 2} + 1.$$

3. (i) $2x + 2y = 1$. (ii) Impossible, if $a, b \neq 0$ then if (x, y) is a solution, so is $(x + b, y - a)$. If $a = 0$ (or $b = 0$) then if $bx = c$ has a solution then (x, y) is a solution for any y. (iii) $x + y = 1$.

4. Let $S = \{1, \ldots, x\}$ and for each $n \in S$ write $n = \prod_i p_i^{\alpha_i}$ where p_j is prime less than x for each j. It is clear that $\alpha_i \leq \frac{\log x}{\log 2}$ because $n < x$ and $p \geq 2$ so consider the number of integers of the form $\prod_i p_i^{\alpha_i}$ with $\alpha_i \in \{0, \ldots, \frac{\log x}{\log 2}\}$ so there are at most $A = \left(1 + \frac{\log x}{\log 2}\right)^{\pi(x)}$ of them so $x \leq A$.

   Take logarithm on both sides so we only need to check that $1 + \frac{\log x}{\log 2} < 2\log x$ for $x \geq 8$.

5. Suppose $a > 2$ then $a - 1 > 1$ is a proper factor of $a^n - 1$. If $n = pq$ where $p, q > 1$ then $a^p - 1$ is a proper factor. The converse is not true, for example $2^{11} - 1 = 23 \times 89$.

6. Let p be a prime factor of $2^q - 1$. Then

   $$2^q \equiv 1 \bmod p, \text{ and } 2^{p-1} \equiv 1 \bmod p \text{ by FLT}$$

   and since q is a prime so $q\big|p - 1$. Since $2^q \equiv 1 \bmod p$ so

   $$\left(2^{\frac{q+1}{2}}\right)^2 = 2^{q+1} \equiv 2 \bmod p$$

so 2 is a square mod p which implies $p \equiv \pm 1 \bmod 8$. Then for 2^{11} the prime factor is 1 mod 11 and ± 1 mod 8 so the first one to try is 23 and so we check it is 23×89.

Here is an elementary proof for the fact that if 2 is a square mod p then $p \equiv \pm 1 \bmod 8$. Let $s = \frac{p-1}{2}$ and if $2 \equiv x^2 \bmod p$ for some x then $2^s \equiv x^{p-1} \equiv 1 \bmod p$. Let

$$\Lambda = (-1) \cdot 2 \cdot (-3) \cdots = \prod_{i=1}^{s} (-1)^i i = s!(-1)^{\frac{s(s+1)}{2}}.$$

Then for each odd integer which appear in the product above, observe that

$$2s = p-1 \equiv -1 \bmod p, 2(s-2) = p-3 \equiv -3 \bmod p, \cdots, 2(s-i) = 2s-2i \equiv -1-2i \bmod p, \cdots$$

so when we consider Λ mod p we can replace each odd integers by some even numbers between s and $p-1$, and so

$$\Lambda \equiv 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv 2^s s! \equiv s! \bmod p$$

using $2^s \equiv 1 \bmod p$. Therefore,

$$s!(-1)^{\frac{s(s+1)}{2}} \equiv 2^s s! \bmod p$$

and so $(-1)^{\frac{s(s+1)}{2}} = 1$ so $p \equiv \pm 1 \bmod 8$.

7. Let $\sigma(n) = \sum_{d|n} d$ and we know σ is multiplicative. Suppose $n = 2^{q-1}(2^q - 1)$ then

$$\sigma(n) = \sigma(2^{q-1})\sigma(2^q - 1) = (2^q - 1)(2^q) = 2n.$$

Conversely, if n is perfect, i.e. $\sigma(n) = 2n$, and as n is even we write $n = 2^{q-1}m$ for some odd integer m. Then $\sigma(n) = (2^q - 1)\sigma(m) = 2n = 2^q m$. As $2^q - 1$ is coprime to 2^q so $2^q - 1$ divides m and write $m = (2^q - 1)k$. Then we have

$$\sigma((2^q - 1)k) = 2^q k.$$

Clearly $(2^q - 1)k$ and k are two distinct factors of $(2^q - 1)k$ and the sum of them is $2^q k$. So the above equality suggests that these two are the only factors of $(2^q - 1)k$ and so $k = 1$ (otherwise 1 is another factor) and $2^q - 1$ is a prime.

8. Suppose we only have finitely many of them, and let p be the largest of them. Let $n = 2^2 \cdot 3 \cdot 5 \cdots p - 1$, then n has a prime factor q which is congruent to 3 mod 4 because n is 3 mod 4. Also q is coprime to any prime less than or equal to p, so $q > p$ which is a contradiction.

9. 1973.

10. This reduces to $x \equiv 337 \bmod 900$ and $x \equiv 808 \bmod 841$ so we have $x \equiv 58837 \bmod 900 \times 841$.

11. Use CRT to construct a solution of

$$x \equiv 0 \bmod 4, x + 1 \equiv 0 \bmod 9, \ldots, x + i \equiv 0 \bmod p_i^2, \ldots$$

where $1 \leq i \leq 100$ and p_i is the ith prime.

12. Both $2, 3$ generate $(\mathbb{Z}/5\mathbb{Z})^\times$ and $2^4 = 1 + 3 \times 5, 3^4 = 1 + 16 \times 5$ and $3, 16$ are prime to 15 so they generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$. In general, if $p > 2$ then following the proof in the notes we know that if g generates $(\mathbb{Z}/p\mathbb{Z})^\times$ and $g^{p-1} = 1 + bp$ where $(b, p) = 1$ then g generates $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all n. For $p = 11, 13$, take 2. $p = 17$, take 3 and $p = 19$ take 2.

13. $A \cong (\mathbb{Z}/2^4\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times$. The order of 3 in $(\mathbb{Z}/2^4\mathbb{Z})^\times$ is 4 and $-1 \notin \langle 3 \rangle$ so by considering the size of the subgroup generated by -1 and 3 we conclude that $(\mathbb{Z}/2^4\mathbb{Z})^\times = \langle -1, 3 \rangle$.

    Define the index of a group G to be the smallest integer n such that $g^n = 1$ for all $g \in G$. Then the index of $(\mathbb{Z}/2^4\mathbb{Z})^\times$ is 4, the index of $(\mathbb{Z}/3^2\mathbb{Z})^\times$ is 6, the index of $(\mathbb{Z}/5\mathbb{Z})^\times$ is 4, the index of $(\mathbb{Z}/7\mathbb{Z})^\times$ is 6 and the index of $(\mathbb{Z}/13\mathbb{Z})^\times$ is 12. So n is the least common multiple of these numbers which is 12.

14. $a^n \equiv 1 \bmod N$ and n is the least such integer because $1 < a^t < N$ for any $t < n$. Thus by Euler's Theorem, $n \big| \phi(N)$. Suppose there are only finitely many $q \equiv 1 \bmod n$ say $q_1, \dots, q_k$. Let $a = nq_1 \cdots q_k$ and $N = a^n - 1$. Then $n \big| \phi(N)$. It is clear that N is coprime to $n, q_1, \dots, q_k$. We write
$$N = \prod_i p_i^{e_i}, \phi(N) = \prod_i p_i^{e_1 - 1}(p_i - 1).$$
    As n is prime to N so $n \nmid p_j$ for any j but $n \big| \phi(N)$ so $n \big| p_j - 1$ for some j and we know p_j cannot be any q_i so this gives a contradiction.

15. This is clear when $n \leq 2$ so we assume $n \geq 3$. We claim that the order of $5 \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ is 2^{n-2}. To prove this, it suffices to show $5^{2^{n-3}} \equiv 1 + 2^{n-1} \bmod 2^n$ (this implies $5^{2^{n-2}} \equiv 1 \bmod 2^n$ and 2^{n-3} is not the order so it must be 2^{n-2}). When $n = 3$ this clearly holds. Suppose this is true for n, then $5^{2^{n-3}} = 1 + 2^{n-1} + a2^n$ for some a and then
$$5^{2^{n-2}} = \left(5^{2^{n-3}}\right)^2 = (1 + 2^{n-1} + a2^n)^2 = 1 + 2^n + b2^{n+1}$$
    where $b = a^2 2^{n-1} + 2a + a2^{n-1} + 2^{n-3}$. Therefore $5^{2^{n-2}} \equiv 1 + 2^n \bmod 2^{n+1}$ so by induction we have proved our claim.

    Now consider the cyclic subgroup generated by 5. Since 5 has order 2^{n-2} so the cyclic subgroup has size 2^{n-2}, and each element in the subgroup must be 1 mod 4, which is in the kernel $(\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$. But there are 2^{n-2} integers in $\{1, \dots, 2^n\}$ which are 1 mod 4 and so the cyclic subgroup generated by 5 is exactly the set of integers which are 1 mod 4, and so the kernel of the natural map is the cyclic subgroup generated by 5.

    Here is an alternative proof. Let H be the kernel and so H consists of the integers which are 1 mod 4 and so $|H| = 2^{n-2}$. Take an element $1 + 4t \in H$ of order 2. Then we have
$$1 + 8t + 16t^2 \equiv 1 \bmod 2^n$$
    and so $2^n | 8t(1 + 2t)$. But $(1 + 2t, 2) = 1$ so $2^n | 8t$ and so $2^{n-3} | t$. This shows that $2^{n-1} | 4t$ and so $4t = 2^{n-1}c$. If c is odd then $1 + 4t \equiv 1 + 2^{n-1} \bmod 2^n$ and if c is even then $1 + 4t \equiv 1 \bmod 2^n$ so the only element of order 2 in H is $1 + 2^{n-1}$.

    Since H is abelian, it is isomorphic to a product of cyclic groups, say $C_{n_1} \times \cdots C_{n_k}$ where $n_1 \cdots n_k = 2^{n-2}$ and so each n_i is a power of 2 and hence even. Suppose H is not cyclic, then $k \geq 2$. If we write C_{n_i} as $\mathbb{Z}/n_i\mathbb{Z}$, then there is a unique element of order 2 in C_{n_i} which is $\frac{n_i}{2}$. Then $(\frac{n_1}{2}, 0, \cdots, 0)$ and $(0, \cdots, \frac{n_k}{2})$ are two distinct elements of order 2 in H which is a contradiction.