Problem Set 3a

Released: August 27, 2021

1. How many zeros does the integer 100! end with (when written in decimal)?

   Solution: First, note that for any natural number n and any prime p, the highest power of p that divides $n!$ is

   $$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

   (this is sometimes called Legendre's formula or de Polignac's formula). Note that even though this summation extends to infinity, all but finitely many terms of the summation will be non-zero.

   Now, the number of zeros at the end of 100! is equal to the highest power of 10 that divides it. But the highest power of 10 is equal to the smaller of the highest powers of 2 and 5 in 100!. Let us compute both of them:

   $$\begin{aligned} v_2(100!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{100}{2^k} \right\rfloor \\ &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \cdots + \left\lfloor \frac{100}{2^6} \right\rfloor \\ &= 50 + 25 + 12 + 6 + 3 + 1 \\ &= 97 \\ v_5(100!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{100}{5^k} \right\rfloor \\ &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor \\ &= 20 + 4 \\ &= 24 \end{aligned}$$

   Therefore the highest power of 10 in 100! is 24. So 100! ends with 24 zeros.

2. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever n is a positive integer.

   Solution: The statement is FALSE. Take $n = 1601$. Then

   $$\begin{aligned} n^2 - 79n + 1601 &= 1601^2 - 79 \cdot 1601 + 1601 \\ &= 1601 \cdot (1601 - 79 + 1) = 1601 \cdot 1523 \end{aligned}$$

   In fact, it is true that for any non-constant polynomial $p(x)$ with integer coefficients, it is not possible for $p(n)$ to be prime for all natural numbers n (although it is possible for $p(n)$ to be prime for infinitely many natural numbers n; for example, take $p(n) = 4n + 3$).

3. Prove or disprove that for every two positive integers a, b, if an integer linear combination of a and b^2 equals 1, then so does an integer linear combination of a^2 and b.

   Solution: Since there is an integer linear combination of a and b^2 that equates to 1, so $\gcd(a, b^2) = 1$. In particular, a and b^2 have no common prime factor. But b^2 and b have the same set of prime factors, and a^2 and a also have the same set of prime factors. So this means a^2 and b also do not share any common prime factors. Therefore $\gcd(a^2, b) = 1$ as well, which implies there exists an integer linear combination of a^2 and b that equals 1.

   Alternately, one can compute such an integer linear combination explicitly. Suppose there exist integers x and y such that $ax + b^2y = 1$. Then squaring both sides, we get $(ax + b^2y)^2 = 1$. Expanding and grouping the terms appropriately, we get

   $$a^2x^2 + b(2abxy + b^3y^2) = 1.$$

   If $x^2 = x_0$ and $2abxy + b^3y^2 = y_0$, then x_0, y_0 are integers, and the above equation reads

   $$a^2x_0 + by_0 = 1,$$

   so there is an integer linear combination of a^2 and b which equates to 1.

4. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some non negative integer n.

Hint: If m is not a power of 2, then it has an odd factor $k > 1$. Can you factorize $2^{tk} + 1$? You can use the fact that for any integers a, b and positive integer k, it holds that $(a - b)|(a^k - b^k)$. You could prove this fact using strong induction by noting that $a^{k+1} - b^{k+1} = (a^k - b^k)(a + b) - (a^{k-1} - b^{k-1})ab$.

Solution: Consider the contrapositive of the given statement; we want to show that if m is not a non-negative power of 2, then $2^m + 1$ is not an odd prime.
If m is not a non-negative power of 2, it has an odd factor $k > 1$. Let $m = tk$ for some natural number t. Then $2^m + 1 = 2^{tk} + 1$. But, by the fact in the hint, using $a = 2^t$ and $b = -1$, we have that, for an odd k, $2^t + 1$ is a factor of $2^{tk} - (-1)^k = 2^{tk} + 1$. (This factorization is more explicitly given by $x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots - x + 1)$, with $x = 2^t$, and k odd, where the second factor has an alternating summation.) Also, $k > 1$ and $t \geq 1$, so $1 < 2^t + 1 < 2^m + 1$, so the factor is non-trivial. This means $2^m + 1$ is not a prime, which is what we wanted to show.

5. Recall the *Skippy Clock* from the lecture: It has numbers $0, 1, .., m - 1$ on its dial, and the needle, starting at 0, moves a steps at a time (i.e., hits numbers $0, a, 2a, \dots$). Show that needle will hit exactly all the multiples of $\gcd(a, m)$ that are on the dial.

Hint: You can use the fact that the "one-dimensional lattice" $L(a, m) \triangleq \{au + mv | u, v \in \mathbb{Z}\}$ consists of exactly all the multiples of $\gcd(a, m)$. However, note that in defining $L(a, m)$, u and v can be negative, whereas the clock's needle moves only clockwise.

Solution: Following the hint, it is enough to show that the set of numbers that the needle will hit are exactly all the numbers in $L(a, m) = \{au + mv | u, v \in \mathbb{Z}\}$ that are in the range $[0, m)$.

Now, the numbers hit by the needle are exactly the numbers in the range $[0, m)$ that are of the form $ax - qm$ for some non-negative integers x and q (x being the number of steps taken and q being the number of full laps of the clock completed by then). Thus every number hit is in $L(a, m)$.

Conversely, consider some number d on the dial that is in $L(a, m)$. That is, $d \in [0, m)$ and $d = au + mv$ for some $u, v \in \mathbb{Z}$. We consider two cases:

Case $u \geq 0$: In this case, after moving u times, the needle will be on a number t on the dial, of the form $au - qm$. Then $t \equiv d \pmod{m}$. But since each number on the dial (i.e., each of 0 to $m - 1$) has a different remainder w.r.t. m, it must be the case that $d = t$.

Case $u < 0$: Consider $u' = u - mu = u(1 - m)$. Note that $u' \geq 0$. Hence, after moving u' steps, the needle will be on a number $t = au' - qm = au - amu - qm = d - m(au + q + v)$, for some integer q. Since $t \equiv d \pmod{m}$, and t and d are both numbers on the dial, it must be the case that they are equal.

Thus in either case, the needle hits the number d. Since d was an arbitrary number on the dial that is in $L(a, m)$, we conclude that the needle hits all such numbers.

Thus, the needle hits exactly those numbers on the dial that are in $L(a, m)$.

6. Here is a game you can analyze with what you have learnt in class and always beat me. We start with two positive integers, a, b, written on a blackboard such that $a > b$ and $\gcd(a, b) = 1$. Now we take turns. I'll let you decide who goes first after seeing a, b. At each turn, the player must write a *new* positive integer on the board that is the difference of two numbers that are already there. If a player cannot play, then they lose.

For example, suppose $a = 5$, $b = 3$ and you choose to make the first move. Then your first move must be to play $5 - 3 = 2$. Then I can play $1 = 3 - 2$ (I cannot play $5 - 2 = 3$ as it is already on the board). You can play $5 - 1 = 4$. At this point I cannot make a move, and I lose.

(a) Show that the game must terminate, and when it terminates, every integer in the range $[1, a]$ is on the board.

Solution: Note that no number larger than a can ever be written on the board. (Otherwise, consider the first turn in which a number $x > a$ is written; then $x = y - z$ for two positive numbers already on the board, and hence $y \leq a$, yielding a contradiction as $x \leq y \leq a$.) Thus every turn before the game terminates writes a new integer in the range $[1, a]$; hence the game terminates after at most $a - 2$ turns (two numbers being already on the board).

To prove that all numbers in the range $[1, a]$ must appear on the board before the game terminates, we shall first prove that the number 1 should appear on the board.

Consider the Extended Euclidean algorithm to derive $\gcd(a, b) = 1$. It gives a decreasing sequence of positive numbers of the form $x_0 = a, x_1 = b, x_2 = \text{rem}(x_0, x_1), \dots, x_{i+1} = \text{rem}(x_{i-1}, x_i), \dots, x_n = 1$. Note that

$\text{rem}(x_{i-1}, x_i) = x_{i-1} - qx_i$ for some positive integer q; we shall insert integers $x_{i-1} - x_i, \ldots, x_{i-1} - (q-1)x_i$ between x_i and x_{i+1}. In the resulting decreasing sequence, $z_0 = a, z_1 = b, z_2 = a - b, \ldots, z_{n'} = 1$, every element z_j for $j > 1$ can be obtained as the difference of two previous elements.

Now, if the game terminates before 1 appears on the board, consider the first element z_j in the sequence that does not appear on the board. (There must be such an element since 1 is in the sequence.) Note that $j > 1$ since a, b have to be on the board. So, z_j can be expressed as the difference of two elements before it in the sequence. But since they are all on the board, the game cannot terminate at that point.

Thus when the game terminates, 1 must be on the board.

Now, suppose the game terminates before all integers in the range $[1, a]$ are on the board. Let w be the largest missing number. Note that $w \neq a$ (because a is on the board). Hence $w + 1$ is in the range $[1, a]$ and must be on the board. We also showed above that 1 must be on the board. But this contradicts the assumption that the game has terminated, since w can be written as $(w + 1) - 1$ as the next move. Hence, the game cannot terminate before all numbers in the range $[1, a]$ appear on the board.

(b) Describe a strategy that lets you win this game every time.

Solution: The game will terminate after exactly $a - 2$ moves. So, if a is odd, you shall choose to start the game, and if a is even, you let me start. In either case, you will make the last move, and I will lose the game.

7. A number is said to be *perfect* if it is equal to the sum of its positive divisors, other than itself. The smallest perfect number is 6 (with $6 = 1 + 2 + 3$, where 1, 2, 3 are its divisors, excluding itself). Around 300 B.C., Euclid proved that *if* $2^n - 1$ is a prime number[1] then $(2^n - 1)2^{n-1}$ is a perfect number. Can you prove this result of Euclid?

Solution: If p is a prime number, then by the fundamental theorem of arithmetic, the unique prime factorization of $m = p2^{n-1}$ consists of p and $n - 1$ powers of 2. Then, the positive divisors of m are exactly all the numbers of the form $p^a 2^b$, where a, b are integers, $0 \leq a \leq 1$ and $0 \leq b \leq n - 1$. Hence the sum of all the positive divisors of $m = p2^{n-1}$ (including itself)

$$\sum_{a=0}^{1} \sum_{b=0}^{n-1} p^a 2^b = \sum_{a=0}^{1} p^a (\sum_{b=0}^{n-1} 2^b) = \sum_{a=0}^{1} p^a (2^n - 1) = (2^n - 1)(1 + p)$$

For $p = 2^n - 1$, we have this evaluate to $(2^n - 1)2^n = 2(2^n - 1)2^{n-1} = 2m$. Hence the sum of all positive divisors of m excluding itself equals m, as required to prove.

8. Find all $m \in \mathbb{Z}^+$ such that, for all integers a, b, $a^2 \equiv b^2 \pmod{m}$ iff $a \equiv b \pmod{m}$.

Solution: By definition, $a \equiv b \pmod{m}$ implies that m divides $a - b$. Since $a^2 - b^2 = (a - b)(a + b)$, it follows that m also divides $a^2 - b^2$. Hence, implication in the backward direction follows.

For the forward direction to hold, it must be the case that for all integers a, b whenever m divides $a^2 - b^2$ it must also divide $a - b$. Let us consider the following cases for m :

(a) $m = 1$: The implication holds trivially as 1 divides every integer.

(b) $m = 2$: Assume that 2 divides $a^2 - b^2$. Note that the integers given by $a - b$ and $a + b$, for integer choices of a and b, have the same parity i.e., either both these integers are odd or both are even. To satisfy the hypothesis, it must be the case that $a - b$ is also even as product of two odd numbers cannot be even.

(c) $m > 2$: Consider $a = m - 1$ and $b = 1$. Check that m divides $a^2 - b^2$ but does not divide $a - b$.

We have shown that only for $m \in \{1, 2\}$ it holds that $a^2 \equiv b^2 \pmod{m}$ iff $a \equiv b \pmod{m}$ for all integers a, b.

9. Suppose $m \in \mathbb{Z}^+$. Show that every $a \in \mathbb{Z}_m$ has at most one multiplicative inverse in $\mathbb{Z}_m$.

Solution: Suppose $a, b, c \in \mathbb{Z}_m$ such that $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$. Then we have $b \equiv (ab)b \equiv (ac)b \equiv (ab)c \equiv c \pmod{m}$. Hence all multiplicative inverses of a (if any) are equal to each other.

[1] Such a prime number is called a Mersenne prime. To date, only 51 such numbers are known, the largest of which was discovered in December 2018. The last 17 such discoveries were made by *The Great Internet Mersenne Prime Search* (GIMPS), a project that started in 1996.

10. Suppose $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. Show that there is an integer x such that $ax \equiv b \pmod{m}$ iff $\gcd(a, m)|b$. Describe an algorithm to find a solution when it exists. (You can use the algorithms covered in the lectures.)

Solution: In one direction, if $ax \equiv b \pmod{m}$, then $ax - b = mq$ for some integer q, and hence $b = ax - mq \in L(a, m)$. Since we have seen that every element in $L(a, m)$ is a multiple of $\gcd(a, m)$, so is b.

Conversely, suppose $\gcd(a, m)|b$. Let $d = \gcd(a, m)$. Consider $a' = a/d$, $m' = m/d$. Note that $\gcd(a', m') = 1$. Hence, modulo m', a' has a multiplicative inverse. Let $za' \equiv 1 \pmod{m'}$, where z can be computed using the Extended Euclidean Algorithm. Then $za' = 1 + qm'$ for some integer q, and hence $(b'z)a' = b' + b'qm'$, where $b' = b/d$ is an integer. Now, multiplying throughout by d, we have $(b'z)a = b + (b'q)m$. Thus $x = b'z$ is a solution for $ax \equiv b \pmod{m}$.