

Solutions: Part II – Problem Sheet 2

1. (a) We will use strong induction. (Proof of strong induction: Suppose that the hypotheses are satisfied. If the conclusion is not satisfied, let $m \geq n_0$ be the least natural number such that $P(m)$ is not true. Then $m \neq n_0$ by (1). Also, $P(n)$ is true for all $n \geq n_0, n < m$. So by (2), $P(m)$ is also true, a contradiction.)

By definition $a_1 < 2, a_2 < 4$, and $a_3 < 8$. Set $n_0 = 1$. Let $n \geq n_0 = 1$ and suppose that $a_k < 2^k$ for all $1 \leq k \leq n$. We wish to show that $a_{n+1} < 2^{n+1}$. If $n \leq 2$, then $a_{n+1} < 2^{n+1}$ is already verified above. Suppose that $n \geq 3$. Then $a_{n+1} = a_n + a_{n-1} + a_{n-2} < 2^n + 2^{n-1} + 2^{n-1} = (4 + 2 + 1) \cdot 2^{n-1} < 8 \cdot 2^{n-1} = 2^{n+1}$. So by strong induction, $a_n < 2^n$ for all n .

- (b) We prove this by induction on n . For $n = 0$ it is obvious: we have only 1 person, no people are eliminated, only number 1 remains. Suppose that the result we want holds for 2^n people, i.e. at the end of elimination, only number 1 remains. Take 2^{n+1} people. After eliminating $2, 4, 6, \dots, 2^{n+1}$, we are left with 2^n people and beginning with the first again, the same as before. So by induction, person 1 is the one left at the end.

2. (a) Write $b = a + nq_1$ and $d = c + nq_2$ which we can do by Proposition 1.2.6 from lecture. Then adding equalities, we get $b + d = a + c + nq_1 + nq_2 = a + c + n(q_1 + q_2)$. This shows that $a + c = b + d \pmod{n}$, again by Proposition 1.2.6 from lecture.
- (b) Similarly, multiplying, we get $bd = (a + nq_1)(c + nq_2) = ac + naq_2 + ncq_1 + n^2q_1q_2$. Thus, $bd = ac + n(aq_2 + cq_1 + nq_1q_2)$, and so $ac \equiv bd \pmod{n}$, again by Proposition 1.2.6.
3. (a) $\gcd(4567, 58) = 1, \gcd(2590, 2018) = 2, \gcd(345, 8900) = 5, \text{lcm}(91, 252) = 3276, \text{lcm}(32, 98) = 1568$.
- (b) $\gcd(a, b) = d$. If $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, this means that $\frac{a}{d}, \frac{b}{d}$ have no common divisors except 1. We prove the result by contradiction. Assume that there exists $c \in \mathbb{Z}, c > 1$, such that $c \mid \frac{a}{d}, \frac{b}{d}$. Then there exists $k, l \in \mathbb{Z}$, such that $\frac{a}{d} = kc$ and $\frac{b}{d} = lc$ or in other words $a = cdk$ and $b = cd़l$. Therefore cd is a common divisor of a and b and $dc > d$, since $c > 1$. But this is a contradiction to the fact that d is the greatest common divisor, hence $c = 1$ is the only divisor of $\frac{a}{d}$ and $\frac{b}{d}$.
4. (a) i. We prove this by induction on $N = \sum_i r_i + \sum_j s_j$. If i is such that $p_i \notin \{q_1, \dots, q_n\}$, then we claim that $p_i \mid a$ but $p_i \nmid b$. The first statement is clear. By induction, $p_i \mid b$ implies $p_i \mid q_j$ for some j , hence $p_i = q_j$ as they are primes. So $p_i \nmid b$. But now it is impossible that $a \mid b$, as if that were true, $p_i \mid b$. So, $a \mid b$ only if $q_j = p_i$ for some j . Fix this j . Since a and b are both multiples of p_i , we have $a \mid b$ if and only if $a/p_i \mid b/p_i$. But by induction, since a/p_i and b/p_i have obvious prime factorisations (reducing an exponent by one and possibly eliminating a prime), we have $a/p_i \mid b/p_i$ if and only if for all $i' \neq i$, there exists j' with $q_{j'} = p_{i'}$ and $s_{j'} \geq r_{i'}$, and also $r_i - 1 \leq s_j - 1$. But this is equivalent to the desired condition.
- ii. First of all, it is clear that a and b are both multiples of the RHS of the gcd equation, by multiplying by the remaining primes with multiplicities. Suppose that $c \mid a, c \mid b$. Then, the prime factorisation of c must see at most the primes p_i with powers at most r_i . It is therefore a factor of the RHS of the gcd equation. This proves the formula.
- Similarly, if c is a multiple of both a and b , then the prime factorisation of c includes at least the primes with exponents in the lcm-equation. But also, this is obviously a multiple of both a and b .

- (b) It can be shown easily that $\max(x, y) + \min(x, y) = x + y$ for any integer x and y . The results then follows immediately from the previous part.
5. (a) $a \equiv a' \pmod{n}$ is equivalent to $a = a' + kn$ for some integer k and $b \equiv b' \pmod{n}$ is equivalent to $b = b' + ln$ for some integer l . Hence $a + b = (a' + b') + (k + l)n$ which yields the result.
- (b) Similarly $a \cdot b = a'b' + (a'l + b'l + k + l)n$, which finishes the proof.
6. (a) $a \equiv b \pmod{n}$ is equivalent to $n|a - b$. We want to show that $a^k \equiv b^k \pmod{n}$ or in other words that $n|a^k - b^k$. We have

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$$

by the binomial formula. Hence $a - b|a^k - b^k$ and finally by transitivity of divisibility since $n|a - b$ we get $n|a^k - b^k$.

- (b) $m = 2k + 1$ since m is odd. Therefore

$$\begin{aligned} A &= \left\{ -\frac{2k+1-1}{2}, -\frac{2k+1-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2} \right\} \\ &= \{-k, -(k-1), \dots, -1, 0, 1, \dots, k-1, k\} \end{aligned}$$

But $-k \equiv k+1 \pmod{m}$ (since $-k - k - 1 = -2k - 1 = -m$ and $m|-m$). Similarly $-(k-1) \equiv k+2 \pmod{m}$ and it is easy to show that $-(k-j) \equiv k+j+1$, $0 \leq j \leq k-1$. Therefore $A = \{0, 1, \dots, k, k+1, \dots, 2k = m-1\}$ which is exactly the set of least nonnegative residues modulo n .

7. (a) This was done in the lecture!
- (b) i. Assume there exists a particular solution (x_0, y_0) . Then $ax_0 + by_0 = c$. Subtracting from the original equation we get

$$a(x - x_0) - b(y - y_0) = 0. \quad (1)$$

Consider now $d = \gcd(a, b)$, since d is a divisor of both a and b we can divide on both sides and get $\frac{a}{d}(x - x_0) - \frac{b}{d}(y - y_0) = 0$. We know from question 3(b) that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, hence $\frac{a}{d}$ does not divide $\frac{b}{d}$ and therefore $\frac{a}{d}$ has to divide $(y - y_0)$. This means that for any $y \in \mathbb{Z}$, there exists a $k \in \mathbb{Z}$, such that

$$y = k \frac{a}{d} + y_0.$$

Replacing now in equation (1) we get that $(x_0 + \frac{b}{d}k, y_0 + \frac{a}{d}k)$ is a solution for any integer k and that therefore there are infinitely many solutions.

- ii. Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$. Therefore $d|ax + by$, for all $x, y \in \mathbb{Z}$. Hence either $d|c$ or there are no solutions.
- iii. If d does not divide c we already know that there is no solution. Assume now that $d|c$. Then there exists an integer k , such that $c = kd$. But since $d = \gcd(a, b)$, by part a) there exists integers s and t , such that $as + bt = d$. Multiplying by k we get $ksa + ktb = c$ and $(x_0 = ks, y_0 = kt)$ is a particular solution. We conclude using part i).
8. (a) i. Since $ax \equiv b \pmod{n}$, by definition $n|ax - b$, and there exists an integer y , such that $ny = ax - b$, or in other words we get an equation of the type $ax + (-n)y = b$. So by the previous question, either it has no solution if $d = \gcd(a, n)$ does not divide b , or it has infinitely many solutions of the form $(x_0 + \frac{n}{d}k, y_0 + \frac{a}{d}k)$ otherwise, with (x_0, y_0) a particular solution.

- ii. We just saw that the set of solutions of the equivalent equation is $(x_0 + \frac{n}{d}k, y_0 + \frac{a}{d}k)$. If two solutions are congruent then $x_0 + \frac{n}{d}k_1 \equiv x_0 + \frac{n}{d}k_2 \pmod{n}$ or in other words $\frac{n}{d}k_1 \equiv \frac{n}{d}k_2 \pmod{n}$. This means that $n|\frac{n}{d}k_1 - \frac{n}{d}k_2 = \frac{n}{d}(k_1 - k_2)$. Therefore there exists an integer l such that $ln = \frac{n}{d}(k_1 - k_2)$. But $\frac{n}{d}|n$ (since $d \cdot \frac{n}{d} = n$). Hence dividing by $\frac{n}{d}$ on both sides one gets $ld = k_1 - k_2$ and finally $k_1 \equiv k_2 \pmod{d}$. Consequently the non-congruent solutions are given by the set

$$\{x_0 + \frac{n}{d}k | k \in \{0, 1, 2, \dots, d-1\}\}.$$

- (b) $18x \equiv 30 \pmod{42}$. $\gcd(18, 42) = 6$, so the equation has exactly 6 incongruent solutions. Now by definition $42|18x - 30$, hence 4 is a solution, and by question 4, the solutions are given by the set $\{4 + \frac{42}{6}k | k \in \{0, 1, 2, 3, 4, 5\}\} = \{4, 11, 18, 25, 32, 39\} \pmod{42}$. $6x \equiv 7 \pmod{8}$: $\gcd(6, 8) = 2$ and 2 do not divide 7. Hence the equation has no solutions.
 $3x \equiv 7 \pmod{4}$. Here $\gcd(3, 4) = 1$, which divides 7. Therefore the equation has exactly one solution. Moreover $4|3x - 7$, and therefore 1 is the only solution.