

Problem 1 (a) Find $\gcd(735, 675)$.
 (b) Find $x, y \in \mathbb{Z}$, $735x + 675y = \gcd(735, 675)$.

Solution.

$$(a) \quad 735 = 1(675) + 60, \quad 675 = 11(60) + 15, \quad 60 = 4(15).$$

Therefore, $\gcd(735, 675) = 15$.

(b)

$$15 = 675 - 11(60) = 675 - 11(735 - 675) = (-11)735 + 12(675).$$

Problem 2 In this problem we consider the gcd of three numbers, instead of the usual two. For example, for the numbers 6, 10, 15 any two have a non-trivial common factor, but the three have no non-trivial common divisor. Given natural numbers a, b, c prove that $\gcd(a, b, c) = 1$ if and only if $\gcd(\gcd(a, b), c) = 1$.

Solution. Let $L = \gcd(a, b, c)$ and $R = \gcd(\gcd(a, b), c)$. Clearly, L divides a, b and c . Therefore, L divides $\gcd(a, b)$ and c (in class we concluded this from the Thm: $\exists x, y \in \mathbb{Z}, ax + by = \gcd(a, b)$). Hence, by the same Thm, L divides R . On the other hand, R divides $\gcd(a, b)$ and c . Therefore, R divides a, b and c . Therefore, R divides L . Therefore, $R = L$.

Problem 3 If $A, B, G \subseteq U$ and $A \cap G \subseteq B \cap G$ and $A \cap G^c \subseteq B \cap G^c$, then $A \subseteq B$.

Solution. Fix $x \in A$. We'll show that $x \in B$. There are two cases to consider: $x \in G$ and $x \in G^c$. If $x \in G$ then, since we already assumed that $x \in A$, we have $x \in A \cap G$. By the hypothesis we have $x \in B \cap G \subseteq B$. Similarly, if $x \in G^c$ then, since we already assumed that $x \in A$, we have $x \in A \cap G^c$. By the hypothesis we have $x \in B \cap G^c \subseteq B$. In either case we have $x \in B$.

Problem 4 Find $x \in \mathbb{N}$, $0 \leq x < 30$ with $x \equiv 417^{249} \pmod{30}$.

Solution. $417 \equiv 13 \pmod{30}$, so $417^{249} \equiv -(3^{249}) \pmod{30}$. We'll now compute mod 3 and mod 10 separately. In the first case we get 0, which is congruent to -3 . In the second case, since $\gcd(3, 10) = 1$ and $\phi(10) = 4$, we know $3^4 \equiv 1 \pmod{10}$. Hence,

$$-(3^{249}) \equiv -(3^4)^{62}3 \equiv -3 \pmod{10}.$$

Therefore, in either case we have $-(3^{249}) \equiv -3$. Hence, $-(3^{249}) \equiv -3 \pmod{30}$. And, $-3 \equiv 27 \pmod{30}$.

Problem 5 Solve

$$x \equiv 1 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Solution. 1, 6, 11, 16, 21, 26, 31 are among the numbers congruent to 1 mod 5. 3, 10, 17, 27, 31 are among the numbers congruent to 3 mod 7. In particular 31 satisfies both.

Problem 6 If p and q are distinct primes and $n = pq$, prove that for all $a \in \mathbb{N}$, $a^{\phi(n)+1} \equiv a \pmod{n}$. **Hint:** Recall that $\phi(pq) = (p-1)(q-1)$.

Solution. We'll compute $a^{\phi(n)+1} \pmod{p}$ and also \pmod{q} . The arguments are similar. We first notice that if $a \equiv 0 \pmod{p}$, then both sides are congruent to 0 and therefore the two sides are congruent. If $a \not\equiv 0 \pmod{p}$, then $\gcd(a, p) = 1$ and hence by FLT

$$a^{\phi(n)+1} \equiv (a^{p-1})^{q-1} a \equiv 1 \cdot a \equiv a \pmod{p}.$$

Problem 7 Prove that for all $n \geq 1$, $\sum_{j=1}^n \frac{1}{j^2} \leq 2 - \frac{1}{n}$.

Solution. We prove this by induction. It is an equality for $n = 1$. So, assume it is true for n and we'll prove:

$$\sum_{j=1}^{n+1} \frac{1}{j^2} \leq 2 - \frac{1}{n+1}.$$

$$\sum_{j=1}^{n+1} \frac{1}{j^2} = \sum_{j=1}^n \frac{1}{j^2} + \frac{1}{(n+1)^2} \leq (\text{by IH}) 2 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

We want to show that this last quantity is less than or equal to $2 - \frac{1}{n+1}$. After cancelling the 2 and rearranging terms we are left to show $\frac{1}{n+1} + \frac{1}{(n+1)^2} \leq \frac{1}{n}$. Multiplying both sides by $n(n+1)^2$ in order to clear all fractions, we must prove that $n(n+1) + n \leq (n+1)^2$, which is clear.

Problem 8 Assume that X has at least two points. Let $f : X \rightarrow Y$ be onto, $C \subsetneq Y$ and $z \in C$. Define

$$F(x) = \begin{cases} f(x) & \text{if } f(x) \in C \\ z & \text{otherwise.} \end{cases}$$

Prove that F is not 1-1.

Solution. First notice that since f is onto, there exists a point, $u \in X$ with $f(u) = z$. But then $F(u) = f(u) = z$. Since C is not all of Y there is a point in C^c , let's call it w . Again, since f is onto there is a point $v \in X$ such that $f(v) = w$. Since $w \in C^c$, $F(v) = z$. But u can't be equal to v since $f(u) = z \in C$ and $f(v) = w \in C^c$. Nonetheless, $F(u) = z = F(v)$. So, F is not 1-1.