Solutions for first midterm

Lennart Meier

September 26, 2019

For each problem I give one possible approach. There might be other solutions. Please write to me if you find any typos or have other remarks.

Problem 1 (10 points)**.** *For the following two equations, decide whether they have solutions with $x, y \in \mathbb{Z}$. If yes, give two different pairs (x, y) of solutions.*

(a) $447x + 408y = -3$

(b) $447x + 408y = 7$

Decide furthermore if the system of congruences

$$\begin{aligned} a &\equiv -3 \mod 447 \\ a &\equiv 7 \mod 408 \end{aligned}$$

has a solution $a \in \mathbb{Z}$ and if yes, give such a solution.

Solution: We use the Euclidean algorithm.

$$\begin{aligned} 447 &= 408 + 39 \\ 408 &= 10 \cdot 39 + 18 \\ 39 &= 2 \cdot 18 + 3 \end{aligned}$$

In particular, we see that $\gcd(447, 408) = 3$ and thus that $447x + 408y = 7$ does not have a solution as 3 does not divide 7. In contrast, the equation (a) has a solution. We write

$$3 = 39 - 2 \cdot 18 = 39 - 2 \cdot (408 - 10 \cdot 39) = -2 \cdot 408 + 21 \cdot (447 - 408) = 21 \cdot 447 - 23 \cdot 408.$$

Thus, $(-21) \cdot 447 + 23 \cdot 408 = -3$. All other solutions are of the form $(-21 + 408k) \cdot 447 + (23 - 447k) \cdot 408 = -3$.

The system of congruences does not have a solution. Indeed, the first congruence implies that $3|a$, while the second implies that a leaves the residue 1 when dividing by 3.

Problem 2 (10 points)**.** *Let a be an arbitrary integer.*

(a) Compute the remainder of a^{36} if we divide by 36*.*

(b) Show that $a^{36} - 1$ is not a prime number.

Solution: (a) We first consider the remainder of a^{36} when dividing by 4 and 9 respectively.

Note that $\phi(4) = 2$ and $\phi(9) = 6$. Thus, $\phi(4)|36$ and $\phi(9)|36$. Euler's theorem implies hence that if a is odd that $a^{36} \equiv 1 \mod 4$. Likewise if a is not divisible by 3, then $a^{36} \equiv 1 \mod 9$.

If a is even, then clearly a^{36} is divisible by 4 and thus $a^{36} \equiv 0 \mod 36$. Likewise, if $3|a$, then $a^{36} \equiv 0 \mod 9$.

By the Chinese remainder theorem, the residues $\mod 4$ and $\mod 9$ determine the residue $\mod 36$ completely. We obtain:

- If a odd and not divisible by 3, then $a^{36} \equiv 1 \mod 36$.
- If a odd and divisible by 3, then $a^{36} \equiv 9 \mod 36$ as $9 \equiv 1 \mod 4$ and $9 \equiv 0 \mod 9$.
- If a even and not divisible by 3, then $a^{36} \equiv 28 \mod 36$ as $28 \equiv 0 \mod 4$ and $28 \equiv 1 \mod 9$.
- If a is even and divisible by 3, then $a^{36} \equiv 0 \mod 36$.

Solution for b: For $a^{36}-1$ to be a prime number, it must be positive; thus $a > 1$. In this case, both $a^{18} - 1$ and $a^{18} + 1$ are bigger than 1. Thus the factorization $a^{36} - 1 = (a^{18} - 1)(a^{18} + 1)$ implies that $a^{36} - 1$ is not prime.

Problem 3 (10 points)**.** *Recall that the sum of positive divisors $\sigma(n)$ of a natural number n with prime factorization $p_1^{k_1} \cdots p_r^{k_r}$ with $p_1 < \cdots < p_r$ equals*

$$\prod_{i=1}^{r} \frac{p^{k_i+1} - 1}{p_i - 1}.$$

Give a similar formula for

$$\sum_{0<d|n} d^2.$$

Solution: The set of divisors of n is $\{p_1^{l_1} \cdots p_r^{l_r} : 0 \le l_i \le k_i\}$. Thus

$$\begin{aligned}\sum_{0<d|n} d^2 &= \sum_{0\le l_1\le k_1} \cdots \sum_{0\le l_r\le k_r} (p_1^{l_1} \cdots p_r^{l_r})^2 \\ &= \prod_{i=1}^{r} \sum_{l_i=0}^{k_i} p^{2l_i} \\ &= \prod_{i=1}^{r} \frac{(p^2)^{l_i+1} - 1}{p_i^2 - 1}\end{aligned}$$