Concepts in Abstract Mathematics
MAT246 LEC0101 Winter 2020
Midterm Exam
Solutions

1. Prove that there is no largest prime number.

Solution. We want to show that if p is prime, then there is another prime $q > p$. Let $M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p + 1$, where the first term is the product of all the primes less than or equal to p. Since every natural number greater than 1 has a prime divisor, there exist a prime q dividing M. Then, $q \neq 2, 3, 5, 7, 11, \ldots, p$, since the remainder of the division of M by any of those numbers is 1. Hence, q is not equal to any of the primes less than or equal to p, so $q > p$.

2. (a) State the Well-Ordering Principle.

(b) State the Principle of Mathematical Induction.

(c) Prove the Principle of Mathematical Induction from the Well-Ordering Principle.

Solution.

(a) Every non-empty subset of $\mathbb{N}$ has a smallest element.

(b) Let S be a subset of $\mathbb{N}$ with the properties that

(A) $1 \in S$, and

(B) if $k \in S$, then $k + 1 \in S$.

Then, $S = \mathbb{N}$.

(c) Let S be a subset of $\mathbb{N}$ satisfying (A) and (B). We want to show that $S = \mathbb{N}$. Equivalently, we want to show that if $T = \{n \in \mathbb{N} : n \notin S\}$ then T is empty. Suppose, by contradiction, that T is not empty. Then, by the Well-Ordering Principle, T has a smallest element $t \in T$. Now, $1 \in S$ by (A) so $1 \notin T$ and hence $t \neq 1$. Thus, $t - 1 > 0$, so $t - 1 \in \mathbb{N}$. Since t is the smallest element of T and $t - 1 < t$, we have $t - 1 \notin T$ so $t - 1 \in S$. But then by (B) this implies that $t = (t - 1) + 1 \in S$, so $t \notin T$, contradicting that $t \in T$. Therefore, T has no smallest element, so T is empty and hence $S = \mathbb{N}$.

3. Prove that there are infinitely many natural numbers n which cannot be written as $n = x^3 + y^3$ for some integers x, y.

Solution. [Note: This is very similar to Q4 in Problem Set 1.]

We claim that if $n \equiv 4 \pmod 7$, then n cannot be written as $n = x^3 + y^3$ for $x, y \in \mathbb{Z}$. Hence, all the numbers of the form $n = 4 + 7m$, for $m \in \mathbb{N}$, have the desired property. To prove the claim, it suffices to show that if $x, y \in \mathbb{Z}$, then $x^3 + y^3 \not\equiv 4 \pmod 7$. We have

$$\begin{aligned}
0^3 &\equiv 0 \pmod 7\\
1^3 &\equiv 1 \pmod 7\\
2^3 &\equiv 1 \pmod 7\\
3^3 &\equiv -1 \pmod 7\\
4^3 &\equiv 1 \pmod 7\\
5^3 &\equiv -1 \pmod 7\\
6^3 &\equiv -1 \pmod 7,
\end{aligned}$$

so $x^3 + y^3 \equiv r + s \pmod 7$ for some $r, s \in \{-1, 0, 1\}$. Thus, $x^3 + y^3 \equiv t \pmod 7$, for some $t \in \{-2, -1, 0, 1, 2\}$. Since $-2 \equiv 5 \pmod 7$ and $-1 \equiv 6 \pmod 7$, we showed that $x^3 + y^3 \equiv t \pmod 7$ for some $t \in \{0, 1, 2, 5, 6\}$. In particular, $x^3 + y^3 \not\equiv 4 \pmod 7$.

4. (a) State Wilson's Theorem.

(b) Use Wilson's Theorem to prove that $2 \cdot (p-3)! \equiv -1 \pmod p$ for all primes $p \geq 4$.

(c) Use (b) to find all primes $p \geq 4$ such that p divides $36 + 2 \cdot (p-3)!$.

Solution.

(a) If p is prime then $(p-1)! + 1 \equiv 0 \pmod p$.

(b) Since $p \equiv 0 \pmod p$, we have

$$\begin{aligned}
(p-1)! &\equiv (p-1) \cdot (p-2) \cdot (p-3)! &&\pmod p\\
&\equiv (-1) \cdot (-2) \cdot (p-3)! &&\pmod p\\
&\equiv 2 \cdot (p-3)! &&\pmod p.
\end{aligned}$$

By Wilson's Theorem, $(p-1)! + 1 \equiv 0 \pmod p$ so $(p-1)! \equiv -1 \pmod p$ and hence

$$2 \cdot (p-3)! \equiv (p-1)! \equiv -1 \pmod p.$$

(c) Let p be prime. Note that $p \mid 36 + 2 \cdot (p-3)!$ if and only if $36 + 2 \cdot (p-3)! \equiv 0 \pmod p$. By (b), $36 + 2 \cdot (p-3)! \equiv 36 - 1 \equiv 35 \pmod p$, so p divides $36 + 2 \cdot (p-3)!$ if and only if $p \mid 35$. Since the prime factorization of 35 is $35 = 5 \cdot 7$, we get that p divides $36 + 2 \cdot (p-3)!$ if and only if $p = 5$ or $p = 7$.

5. Consider the RSA method with the primes $p = 5$ and $q = 13$.

(a) Only one of the following numbers is a valid encryptor. Which one and why?
$$E = 3, \qquad E = 11, \qquad E = 14.$$

(b) Use the Euclidean Algorithm to find a decryptor D corresponding to the encryptor E found in part (a) and such that $0 < D < (p-1)(q-1)$.

(c) A number M such that $0 \le M < pq$ has been encrypted with the encryptor E found in part (a) and the result is $R = 8$. Use the decryptor D found in part (b) to recover M.

Solution.

(a) $E = 11$ since this is the only number relatively prime to $(p-1)(q-1) = 4 \cdot 12 = 48$.

(b) The Euclidean Algorithm gives

$$\begin{aligned} 48 &= 11 \cdot 4 + 4 \\ 11 &= 4 \cdot 2 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

so

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (11 - 4 \cdot 2) \cdot 1 \\ &= 4 \cdot 3 - 11 \cdot 1 \\ &= (48 - 11 \cdot 4) \cdot 3 - 11 \cdot 1 \\ &= 48 \cdot 3 - 11 \cdot 13. \end{aligned}$$

Hence,
$$11 \cdot (48m - 13) = 1 + 48 \cdot (11m - 3)$$
for all $m \in \mathbb{Z}$. We can take $m = 1$, so

$$D = 48 - 13 = 35$$

is a valid decryptor.

(c) Note that $8^2 = 64 \equiv -1 \pmod{65}$, so

$$\begin{aligned} R^D = 8^{35} = (8^2)^{17} \cdot 8 &\equiv (-1)^{17} \cdot 8 \pmod{65} \\ &\equiv -8 \pmod{65} \\ &\equiv 57 \pmod{65}. \end{aligned}$$

Hence, $M = 57$.

6. (a) Prove that if p is a prime number, then $\sqrt{p}$ is irrational.
(b) Use (a) to prove that $\sqrt{5}+\sqrt{7}$ is irrational.

Solution.

(a) Suppose, by contradiction, that $\sqrt{p}$ is rational. Then, $\sqrt{p} = \frac{m}{n}$ for some $m, n \in \mathbb{N}$. Moreover, by dividing by their greatest common divisor if necessary, we can assume that m and n are relatively prime. Then, $p = (\sqrt{p})^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$, so $pn^2 = m^2$. In particular, $p \mid m^2$. Since p is prime, this implies that $p \mid m$. Hence, we can write $m = kp$ for some $k \in \mathbb{N}$. Then, $pn^2 = m^2 = (kp)^2 = k^2p^2$ and by dividing both sides by p, we get $n^2 = k^2p$. In particular, $p \mid n^2$ and again since p is prime this implies that $p \mid n$. But then p is a common divisor of m and n and $p > 1$, contradicting that m and n are relatively prime. Thus, $\sqrt{p}$ is irrational.

(b) Suppose, by contradiction, that $\sqrt{5}+\sqrt{7} = r \in \mathbb{Q}$. Then, $\sqrt{5} = r - \sqrt{7}$ so $5 = (r-\sqrt{7})^2 = r^2 - 2r\sqrt{7} + 7$ and hence

$$\sqrt{7} = \frac{r^2+2}{2r}.$$

But r is rational, so the right-hand side is rational, and this contradicts part (a) since 7 is prime. Thus, $\sqrt{5}+\sqrt{7}$ is irrational.

7. (a) Define the Euler ϕ function.
(b) State Euler's Theorem.
(c) Use (b) to find a multiplicative inverse of 2^{29} modulo 9.

Solution.

(a) For $m \in \mathbb{N}$, $\phi(m)$ is the number of elements of $\{1, \dots, m\}$ that are relatively prime to m.

(b) If m is a natural number greater than 1 and a is a natural number that is relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

(c) We have $\phi(9) = 6$ and $\gcd(2, 9) = 1$, so $2^6 \equiv 1 \pmod{9}$ by Euler's Theorem. Hence,

$$2^{29} \cdot 2 \equiv 2^{30} \equiv (2^6)^5 \equiv 1^5 \equiv 1 \pmod{9},$$

so 2 is a multiplicative inverse of 2^{29} modulo 9.