Solutions to the Term Test, Winter 2014

(1) (8 pts) Prove that there are infinitely many prime numbers of the form $4k+3$.

Hint: If $p_1, p_2, \dots p_n$ are n such primes, look at $4(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1$.

Solution

Suppose there are only finitely many prime numbers of the form $4k+3$. Let $p_1, p_2, \dots p_n$ be all of them.

Let $N = 4(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1$. Obviously, $N \equiv 3 \pmod 4$

Consider its prime factorization $N = q_1 \cdot \dots \cdot q_l$.

Note that N is odd and hence all q_i are odd. We claim that there is at least one i such that $q_i \equiv 3 \pmod 4$. If not then $q_i \equiv 1 \pmod 4$ for all i and hence $N = q_1 \cdot \dots \cdot q_l \equiv 1 \cdot \dots \cdot 1 \equiv 1 \pmod 4$. However, this contradicts the fact that $N \equiv 3 \pmod 4$.

Thus, at least one q_i satisfies $q_i \equiv 3 \pmod 4$. By renumbering q_is we can assume that $q_1 \equiv 3 \pmod 4$.

Next we claim that $q_1 \neq p_j$ for all j. Suppose this is not true and $q_1 = p_j$ for some j. Then q_1 divides N and $q_1 = p_j$ divides $N + 1 = 4(p_1 \cdot p_2 \cdot \dots \cdot p_n)$. Therefore, q_1 divides $N + 1 - N = 1$ and hence $q_1 = 1$. This is a contradiction as all prime numbers are bigger than 1. Thus q_1 is different from all p_j. We also know that $q_1 \equiv 3 \pmod 4$, i.e. it's equal to $4k+3$ for some integer k. This contradicts our original assumption that $p_1, \dots, p_n$ were all possible primes of this form. Therefore, there exist infinitely many prime numbers of the form $4k+3$. $\square$

(2) (8 pts) Using induction prove that for all natural n the following inequality holds:

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots \frac{1}{\sqrt{n}} < 2\sqrt{n}$$

Solution

We prove the inequality by induction. First we check that it holds for $n = 1$. We have that $\frac{1}{\sqrt{1}} = 1 < 2\sqrt{1} = 2$. This verifies the base of induction.

Induction Step. Suppose we have already proved that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots \frac{1}{\sqrt{n}} < 2\sqrt{n}$ for some $n \geq 1$. We need to verify that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} < 2\sqrt{n+1}$.

Using the induction assumption we get $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} < 2\sqrt{n} + \frac{1}{\sqrt{n+1}}$.

Thus, it's enough to prove that $2\sqrt{n} + \frac{1}{\sqrt{n+1}} < 2\sqrt{n+1}$. This is equivalent to $2\sqrt{n} < 2\sqrt{n+1} - \frac{1}{\sqrt{n+1}}$. Since both sides of this inequality are clearly positive it's equivalent to

$$(2\sqrt{n})^2 < (2\sqrt{n+1} - \frac{1}{\sqrt{n+1}})^2 = 4(n+1) + \frac{1}{n+1} - 4, \quad 4n < 4n + 4 + \frac{1}{n+1} - 4 = 4n + \frac{1}{n+1},$$

$$4n < 4n + \frac{1}{n+1}$$

which is true. This proves the induction step. $\square$.

(3) (8 pts) Find the general integer solution of the following equation

$$22x + 74y = 4$$

Solution

First we divide the equation by 2 to get an equivalent one

$$11x + 37y = 2$$

Since $gcd(37, 11) = 1$ there exist integer x, y such that $11x + 37y = 1$. We can find one such pair using the Euclidean algorithm.

$37 = 3 \cdot 11 + 4, 11 = 2 \cdot 4 + 3, 4 = 1 \cdot 3 + 1.$

This gives $4 = 37 \cdot 1 - 11 \cdot 3, 3 = 11 \cdot 1 - 4 \cdot 2 = 11 \cdot 1 - (37 \cdot 1 - 11 \cdot 3) \cdot 2 = 11 \cdot 7 - 37 \cdot 2.$

Lastly from the equality $4 = 1 \cdot 3 + 1$ we get $1 = 4 - 3 = 37 \cdot 1 - 11 \cdot 3 - (11 \cdot 7 - 37 \cdot 2) = 37 \cdot 3 - 11 \cdot 10.$

Multiplying the equality $1 = 37 \cdot 3 - 11 \cdot 10$ by 2 we get $2 = 37 \cdot 6 - 11 \cdot 20.$

Thus $x_0 = -20, y_0 = 6$ satisfy $11x_0 + 37y_0 = 2$. Since $gcd(11, 37) = 1$ the general solution of $11x + 37y = 2$ is $x_0 + 37k, y_0 - 11k$ or $x = -20 + 37k, y = 6 - 11k$ where k is any integer.

(4) (12 pts)

(a) Find

$$1 + 3 + 3^2 + \ldots + 3^{2014} \pmod 7$$

Solution

Let $\Sigma = 1 + 3 + 3^2 + \ldots + 3^{2014}$. Recall that we have a general formula $1 + a + a^2 + \ldots + a^n = \frac{a^{n+1}-1}{a-1}$ for any $a \neq 1$. Using this with $a = 3, n = 2014$ gives $\Sigma = \frac{3^{2015}-1}{2}$.

Next we find $3^{2015} \pmod 7$. Since 7 is prime and does not divide 3 we have that $3^6 \equiv 1$ by Fermat's theorem. Therefore, $3^{6k} \equiv 1 \pmod 7$ for any natural k. Dividing 2015 by 6 with remainder we obtain $2015 = 335 \cdot 6 + 5$. Therefore, $3^{2015} = 3^{335 \cdot 6} \cdot 3^5 \equiv 3^5 \pmod 7 \equiv 3^2 \cdot 3^3 \pmod 7 \equiv 2 \cdot 6 \mod 7 \equiv 5 \pmod 7$. Thus $3^{2015} \equiv 5 \pmod 7$ and $3^{2015} - 1 \equiv 4 \pmod 7$.

By above $\Sigma = \frac{3^{2015}-1}{2}$ so that $2\Sigma \equiv 4 \pmod 7$.

Since $gcd(2, 7) = 1$ the equation $2x \equiv 4 \pmod 7$ has a unique solution mod 7. Obviously, $x \equiv 2 \pmod 7$ works and hence

$\Sigma \equiv 2 \pmod 7$.

(b) Find $40! \pmod{43}$

Solution

Since 43 is prime, by Wilson's theorem, $42! \equiv -1 \pmod{43}$. We can rewrite this as $40! \cdot 41 \cdot 42 \equiv -1 \pmod{43}$. Hence $40! \cdot (-2) \cdot (-1) \equiv -1 \pmod{43}, 2 \cdot 40! \equiv -1 \pmod{43}$. Observe that $2 \cdot 22 = 44 \equiv 1 \pmod{43}$. therefore, multiplying the equality $2 \cdot 40! \equiv -1 \pmod{43}$ by 22 we get $(22 \cdot 2) \cdot 40! \equiv -22 \pmod{43}, 1 \cdot 40! \equiv -22 \pmod{43} \equiv 21 \pmod{43}$.

Answer: $40! \equiv 21 \pmod{43}$.

(5) (8 pts) Prove that $\frac{2+3\sqrt[3]{7}}{11.1}$ is irrational.

Solution

Let us first prove that $x_0 = \sqrt[3]{7}$ is irrational. It's a root of $x^3 - 7 = 0$. Suppose it's rational. Then by the rational root theorem it can be written as $\frac{p}{q}$ where $gcd(p, q) = 1, p| - 7, q|1$. Therefore, $p = \pm 1, \pm 7, q = \pm 1$ which means that the only options for x_0 are $x_0 = \pm 1, \pm 7$. Direct substitution shows that none of these numbers satisfy $x^3 - 7 = 0$ and hence $\sqrt[3]{7}$ is irrational.

Next suppose $x = \frac{2+3\sqrt[3]{7}}{11.1}$ is rational. Then $11.1x = 2 + 3\sqrt[3]{7}$, $\frac{111}{10}x = 2 + 3\sqrt[3]{7}$, $\frac{111}{10}x - 2 = +3\sqrt[3]{7}$, $\frac{\frac{111}{10}x-2}{3} = \sqrt[3]{7}$. Since sums, products and quotients of rational numbers are rational, if x is rational then $\frac{\frac{111}{10}x-2}{3}$ is rational too which means that $\sqrt[3]{7}$ is rational. However, we proved that it's irrational. This is a contradiction and therefore x is irrational.

(6) (8 pts) Two people are communicating using the RSA encryption system. The receiver broadcasts the numbers $N = 69, E = 5$. The sender wants to send a secret message M to the receiver. What is sent is the number $R = 2$.

Decode the original message M.

Solution

We have $N = 69 = 3 \cdot 23$ and $\phi(N) = (3-1)\cdot(23-1) = 44$. In order to decode the message we need to find natural D such that $DE \equiv 1 \pmod N$ or $5D \equiv 1 \pmod{44}$. We can find D using the Euclidean algorithm or we can just observe that $9 \cdot 5 = 45 \equiv 1 \pmod{44}$ so that $D = 9$ works. therefore $M = R^D \pmod N$, $M = 2^9 \pmod{69}$. We compute $2^6 = 64 \equiv -5 \pmod{69}, 2^3 = 8$ and hence $2^9 = 2^6 \cdot 2^3 \equiv -5 \cdot 8 \pmod{69} \equiv -40 \pmod{69} \equiv 29 \pmod{69}$.

Answer: $M = 29$.

(7) (8 pts) Let a, m be natural numbers.

Prove that there exists an integer b such that $ab \equiv 1 \pmod m$ if and only if $gcd(a, m) = 1$.

Solution

Suppose $gcd(a, m) = 1$. Then as a consequence of the Euclidean algorithm there exist integer x, y such that $ax + my = gcd(a, m) = 1$. Then $ax = 1 - my$ which means that $ax \equiv 1 \pmod m$. Therefore $b = x$ satisfies $ab \equiv 1 \pmod m$.

Conversely, suppose there is an integer b such that $ab \equiv 1 \pmod m$. This means that $ab - 1 = mk, ab - km = 1$ for some integer k. Let $d = gcd(a, m)$. Then $a = da', m = dm'$ for some natural a', m'. Hence $1 = ab - km = da'b - kdm' = d(a'b - km')$. This means that d divides 1 and hence $d = 1$. $\square$