Solutions to the Term Test, Winter 2015

(1) (8 pts) Find a mistake in the following "proof".

Claim: for any $n \geq 2$ the sum of any n odd numbers is even.

Proof:

a) The sum of any two odd numbers is even so the claim is definitely true for $n = 2$. This verifies the base of induction.

b) Induction step. Suppose the claim has been proved for some $n \geq 2$. Let us prove it for $n + 1$. Let $a_1, a_2, \ldots, a_{n+1}$ be $n + 1$ odd numbers. Then by the induction assumption $a_1 + a_2$ is even and $a_3 + \ldots + a_{n+1}$ is even. Since the sum of any two even numbers is even we have that $a_1 + a_2 + a_3 + \ldots + a_{n+1} = (a_1 + a_2) + (a_3 + \ldots + a_{n+1})$ is even. $\square$

Solution

The induction step fails for $n = 2$ because the second bracket in the sum $(a_1+a_2)+(a_3+\ldots+a_{n+1})$ equals to $(a_3+\ldots+a_{n+1}) = a_3$ contains only one summand and therefore the induction assumption is not applicable to it.

(2) (8 pts)

Prove that

$$\frac{\sqrt[10]{3} - 17.26}{\sqrt[3]{27} + 11/33}$$

is irrational.

Solution

Suppose $q = \frac{\sqrt[10]{3}-17.26}{\sqrt[3]{27}+11/33}$ is rational. Since $\sqrt[3]{27} = 3$ we can rewrite q as

$$q = \frac{\sqrt[10]{3} - 17.26}{3 + 11/33} = \frac{\sqrt[10]{3} - 17.26}{110/33}$$

Since q is rational so is $\frac{110}{33}q = \sqrt[10]{3} - 17.26$ is rational and hence, $\frac{110}{33}q + 17.26 = \sqrt[10]{3}$ is rational since the sum of two rational numbers is rational and $17.26 = \frac{1726}{100}$ is rational. Thus, $\sqrt[10]{3}$ is rational. Hence it can be written as $\frac{p}{q}$ where $gcd(p, q) = 1$. Since $x = \sqrt[10]{3}$ satisfies $x^{10} - 3 = 0$, by the Rational Root Theorem, we must have $p|3, q|1$. Hence $p = \pm 1, \pm 3$, $q = \pm 1$ and $\frac{p}{q} = \pm 1 \pm 3$. Since $\sqrt[10]{3} > 0$ we only need to consider the possibilities $x = +1, +3$. Plugging them into the equation $x^{10} - 3 = 0$ we see that neither is a root: $1^{10} - 3 = -2 \neq 0$, $3^{10} - 2 > 0$.

This is a contradiction and therefore q is irrational. $\square$.

(3) (8 pts) Find the last two digits of 7^{2002}.

Solution

The last two digits of 7^{2002} are equal to the remainder when 7^{2002} is divided by 100. Thus we need to find $7^{2002} \pmod{100}$.

We have $\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40$. Since $gcd(7, 100) = 1$, by Euler's theorem, $7^{\phi(100)} = 7^{40} \equiv 1 \pmod{100}$.

Therefore, $7^{2002} = 7^{2000} \cdot 7^2 = (7^{40})^{50} \cdot 7^2 \equiv 1 \cdot 49 \equiv 49 \pmod{100}$.

Answer: The last two digits of 7^{2002} are 49.

(4) (10 pts) Prove that if $2^k + 1$ is prime then $k = 2^m$ for some $m \geq 0$.

Hint: If $k = ab$ where b is odd consider the remainder when $2^k + 1$ is divided by $2^a + 1$.

Solution

Suppose k is not a power of 2. Consider its prime factorization $k = p_1 \cdot \ldots \cdot p_n$ where all p_i are prime. Then at least one $p_i \neq 2$. Without loss of generality $p_n \neq 2$. Then p_n is odd as 2 is the only prime number which is even. Also $p_n > 1$.

We have $k = (p_1 \cdot \ldots \cdot p_{n-1}) \cdot p_n = ab$ where $a = p_1 \cdot \ldots \cdot p_{n-1}$ and $b = p_n > 1$ and is odd.

Claim: $2^a + 1$ divides $2^k + 1$. Indeed, we have $2^a \equiv -1 \pmod{2^a + 1}$ and therefore $2^k = (2^a)^b \equiv (-1)^b \equiv -1 \pmod{2^a + 1}$ since b is odd. Therefore, $2^a + 1$ divides $2^k - (-1) = 2^k + 1$ which proves the Claim.

Next observe that $2^a + 1 > 1$ since $a \geq 1$. Also, $2^a + 1 < 2^k + 1$ since $k = ab > a$. This means that $2^k + 1$ is not prime. This is a contradiction and therefore k has no other prime divisors other than 2. $\square$

(5) (8 pts) A message was encoded using the RSA encryption with $N = 35$ and $E = 7$. The encoded message is $R = 33$.

Decode the original message M.

Solution

We have $N = 35 = 5 \cdot 7$. Hence $\phi(N) = (5-1) \cdot (7-1) = 24$. We need to find the decoder D which is a number satisfying $DE \equiv 1 \pmod{24}$ or $7D \equiv 1 \pmod{24}$. By inspection we see that $D = 7$ works because $7 \cdot 7 = 49 \equiv 1 \pmod{24}$. In an RSA encryption process M can be recovered by the formula $M = R^D \pmod{N}$ which in our case gives $M = 33^7 \pmod{35} \equiv (-2)^7 \pmod{35} \equiv -128 \pmod{35} \equiv 12 \pmod{35}$.

Answer: $M = 12$.

(6) (8 pts) Find the remainder when $17^{3^{100}}$ is divided by 20.

Solution

We have $\phi(20) = \phi(2^2 \cdot 5) = (2^2 - 2)(5 - 1) = 8$. Since, $gcd(17, 20) = 1$, by Euler's theorem $17^8 \equiv 1 \pmod{20}$. Therefore, we need to find $3^{100} \pmod 8$. We have $3^2 = 9 \equiv 1 \pmod 8$ and hence $3^{100} = (3^2)^{50} \equiv 1 \pmod 8$. This means that $3^{100} = 8k + 1$ for some natural k. Therefore,

$$17^{3^{100}} = 17^{8k+1} = (17^8)^k \cdot 17 \equiv 1^1 \cdot 17 \equiv 17 \pmod{20}$$

Answer: 17.

(7) (10 pts) Mark **True** or **False**. You **DO NOT** need to justify your answer.

(a) $2014! \equiv -1 \pmod{2015}$
This is false because $2015 = 5 \cdot 403$ and both 5 and 403 are smaller than 2014. Therefore, 2014! is divisible by $5 \cdot 403 = 2015$, i.e $2014! \equiv 0 \pmod{2015}$.
Answer: False.

(b) product of two irrational numbers is always irrational; This is false, for example $\sqrt{2}$ is irrational but $\sqrt{2} \cdot \sqrt{2} = 2$ is rational. **Answer: False**.

(c) every prime number is odd
Answer: False. since 2 is prime and is even.

(d) If $ab \equiv 1 \pmod c$ then $gcd(a, c) = 1$.
This is true. Let $d = gcd(a, c)$. Then $d|a$ and $d|c$. $ab \equiv 1 \pmod c$ means that $ab - 1 = kc$ for some integer k or, equivalently, $1 = ab - kc$. Since $d|a$ and $d|c$ this implies that $d|ab - kc = 1$ and hence $d = 1$.
Answer: True.

(e) If p is prime and $p|a_1 \cdot a_2 \cdot \ldots \cdot a_n$ then $p|a_i$ for some i. This is a corollary of the Fundamental Theorem of Arithmetic.
Answer: True.