Solutions to Practice Final 1

1. (a) What is $\phi(20^{100})$ where ϕ is Euler's ϕ-function?

   (b) Find an integer x such that $140x \equiv 133 \pmod{301}$. Hint: $\gcd(140, 301) = 7$.

Solution

(a) $\phi(20^{100}) = \phi(4^{100} \cdot 5^{100}) = \phi(2^{200} \cdot 5^{100}) = (2^{200} - 2^{199})(5^{100} - 5^{99}) =$
$= 2^{199}(2-1)5^{99}(5-1) = 2^{199} \cdot 5^{99} \cdot 4 = 2^{201} \cdot 5^{99}$

(b) Note that $140 = 2^2 \cdot 5 \cdot 7$ and $301 = 7 \cdot 43$ are prime decompositions. also $133 = 7 \cdot 19$. therefore

$140x \equiv 133 \pmod{301}$ means $7 \cdot 20x \equiv 7 \cdot 19 \pmod{7 \cdot 43}$ and is equivalent to $20x \equiv 19 \pmod{43}$.

Since 43 is prime and it does not divide 20, by the Little Fermat theorem we have that $20^{42} \equiv 1 \pmod{43}$ and hence $20 \cdot 20^{41} \cdot 19 \equiv 19 \pmod{43}$. Therefore we can take $x = 20^{41} \cdot 19$.

2. (a) Prove, by mathematical induction, that $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$ for every natural number n.

   (b) Prove that for p an odd prime (that is, p is a prime that is not equal to 2), $1^p + 2^p + 3^p + ... + (p-1)^p \equiv 0 \pmod{p}$.

Solution

(a) First we check the formula for $n = 1$. we have $1 = \frac{1(1+1)}{2}$ so the formula is true there. suppose the formula is proved for $n \geq 1$ and $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$. Then $1 + 2 + 3 + ... + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$ which means that the formula is true for $n+1$ also. By induction this means that the formula holds for all natural n.

(b) Prove that for p an odd prime (that is, p is a prime that is not equal to 2), $1^p + 2^p + 3^p + ... + (p-1)^p \equiv 0 \pmod{p}$.

By Little Fermat theorem we have that $a^{p-1} \equiv 1 \pmod{p}$ for any $a = 1, \ldots, p-1$. Multiplying this by a gives $a^p \equiv a \pmod{p}$ any $a = 1, \ldots, p-1$. Therefore $1^p + 2^p + 3^p + ... + (p-1)^p \equiv 1 + 2 + \ldots (p-1) \equiv \frac{(p-1)p}{2} \pmod{p}$ by part (a). Note that $p-1$ is even which means that $k = \frac{p-1}{2}$ is an integer. therefore

$$1^p + 2^p + 3^p + ... + (p-1)^p \equiv kp \equiv 0 \pmod{p}$$

3. Prove that for any odd integer a, a and a^{4n+1} have the same last digit for every natural number n.

Solution

If a is odd and is divisible by 5 then the last digit of a is 5. therefore, the last digit of any power of a is also 5 and the statement is clear.

Now suppose $(a, 5) = 1$. Since a is odd this means $(a, 10) = 1$ also. By Euler's theorem $a^{\phi(10)} \equiv 1 \pmod{10}$. we have $\phi(10) = \phi(2 \cdot 5) = (2-1) \cdot (5-1) = 4$. Thus $a^4 \equiv 1 \pmod{10}$. therefore $a^{4k} \equiv 1 \pmod{10}$ for any natural k and hence $a^{4k+1} \equiv a \pmod{10}$ which means that a^{4k+1} and a have the same last digit.

4. Recall that a "perfect square" is a number of the form n^2 where n is a natural number. Show that 9120342526523 is not the sum of two perfect squares. Hint: Consider values modulo 4.

Solution

If $a \equiv 0 \pmod 4$ or $a \equiv 2 \pmod 4$ then $a^2 \equiv 0 \pmod 4$. If $a \equiv 1 \pmod 4$ or $a \equiv 3 \pmod 4$ then $a^2 \equiv 1 \pmod 4$. Thus the only possible values of $a^2 \pmod 4$ or 0 and 1.

Therefore the only possible values $\pmod 4$ for $a^2 + b^2$ are $0 + 0 = 0, 0 + 1 = 1$ and $1 + 1 = 2$.

On the other hand we have $9120342526523 = 91203425265 \cdot 100 + 23 \equiv 23 \equiv 3 \pmod 4$ (we used that $100 \equiv 0 \pmod 4$. thus 9120342526523 can not be written as $a^2 + b^2$.

5. (a) Are there rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$? Justify your answer.

   (b) Prove that $\frac{\sqrt{5}}{\sqrt{2}+\sqrt{11}}$ is irrational.

Solution

(a) Suppose $\sqrt{3} = a + b\sqrt{2}$ where a and b are rational. taking squares of both sides we get $3 = a^2 + 2ab\sqrt{2} + 2b^2, 3 - a^2 - 2b^2 = 2ab\sqrt{2}$. Note that we can not have $a = 0$ since it would mean $\sqrt{3} = b\sqrt{2}, \sqrt{\frac{3}{2}} = b$ is rational. This is easily seen to be impossible. Similarly we can not have $b = 0$ as this would mean that $\sqrt{3} = a$ is rational. Thus $3 - a^2 - 2b^2 = 2ab\sqrt{2}$ means $\sqrt{2} = \frac{3-a^2-2b^2}{2ab}$ is rational. this is impossible and therefore we can not write $\sqrt{3} = a + b\sqrt{2}$ with rational a, b.

(b) Suppose $\frac{\sqrt{5}}{\sqrt{2}+\sqrt{11}} = q$ is rational. then $\sqrt{5} = q(\sqrt{2} + \sqrt{11})$. Note that q can not be equal to zero.
taking squares of both sides we get $5 = q^2(2 + 11 + 2\sqrt{22})$. This means $\frac{5}{q^2} = 13 + 2\sqrt{22}, \sqrt{22} = \frac{5-13q^2}{2q^2}$ is rational. This is a contradiction and hence $\frac{\sqrt{5}}{\sqrt{2}+\sqrt{11}}$ is irrational.

6. (a) What is the cardinality of the set of roots of polynomials with constructible coefficients? Justify your answer.

   (b) Let $\mathbb{N}$ denote the set of all natural numbers. What is the cardinality of the set of all functions from $\mathbb{N}$ to $\{1, 3, 5\}$? Justify your answer.

Solution

(a) Let S be the set of roots of polynomials with constructible coefficients. It's easy to see that $|S| \geq |\mathbb{N}|$. On the other hand, it was proved in class that a root of a polynomial with constructible coefficients is also a root of a polynomial with rational coefficients. Therefore all elements of S are algebraic and hence $|S| \leq |\mathbb{N}|$. By Schroeder-Berenstein this implies that $|S| = |\mathbb{N}|$.

(b) Let $\mathbb{N}$ denote the set of all natural numbers. What is the cardinality of the set S of all functions from $\mathbb{N}$ to $\{1, 3, 5\}$?

First observe that any such function corresponds to a sequence $a_1, a_2, a_3, \ldots$ where each a_i is equal either 1, 3 or 5. Consider the map

$f\colon S \to \mathbb{R}$ given by $f(a_1, a_2, a_3, \ldots) = 0.a_1a_2a_3\ldots$. Clearly f is 1-1 which means that $|S| \leq |\mathbb{R}|$.

On the other hand recall that $|\mathbb{R}| = |P(\mathbb{N})|$ and $P(\mathbb{N})$ is equal to the set of functions from N to $\{0, 1\}$. Since $|\{0, 1\}| \leq |\{1, 3, 5\}|$ we have that $|\mathbb{R}| = |P(\mathbb{N})| \leq |S|$.

By Schroeder-Berenstein theorem this implies that $|S| = |\mathbb{R}|$.

7. Let θ be an angle between 0 and 90 degrees. Suppose that $\cos\theta = \frac{3}{4}$. Prove that $\frac{\theta}{3}$ is not a constructible angle.

Solution

let $x = \cos\frac{\theta}{3}$. Suppose x is constructible. using the formula $\cos(\theta) = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3}$ we see that $4x^3 - 3x = \frac{3}{4}$. therefore $16x^3 - 12x = 3$. If x is constructible then so is $y = 2x$ which must satisfy $2y^3 - 6y = 3, 2y^3 - 6y - 3 = 0$. this is a cubic polynomial with rational coefficients. If it has a constructible root it must have a rational one. Suppose $\frac{p}{q}$ is a rational root of $2y^3 - 6y - 3 = 0$ where p, q are relatively prime integers. Then $p|3$ and $q|2$. Thus the only possibilities for $\frac{p}{q}$ are $\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}$. Plugging those numbers into $2y^3 - 6y - 3$ we see that none of them are roots. This is a contradiction and hence, x is not constructible.

8. For each of the following numbers, state whether or not it is constructible and justify your answer.

   (a) $\cos\theta$ where the angle $\frac{\theta}{3}$ is constructible

(b) $\sqrt[3]{\frac{25}{8}}$

(c) $\sqrt{7+\sqrt{5}}$

(d) $(0.029)^{1/3}$

(e) $\tan 22.5°$

Solution

(a) $\cos(\theta) = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3}$, therefore it's constructible if $\cos\theta$ is.

(b) $\sqrt[3]{\frac{25}{8}} = \frac{\sqrt[3]{25}}{2}$. If it were constructible then so would be $\sqrt[3]{25}$ which is a root of $x^3 - 25 = 0$. This is a cubic polynomial with rational coefficients. If it has a constructible root it must have a rational root which has to be an integer dividing 25. The only possibilities are $\pm1, \pm5, \pm25$. None of these are roots of $x^3 - 25 = 0$ and hence $\sqrt[3]{\frac{25}{8}}$ is not constructible.

(c) $\sqrt{7+\sqrt{5}}$ belongs to F_2 for the tower of fields $\mathbb{Q} = F_0 \subset F_1 = F_0(\sqrt{5}) \subset F_2 = F_1(\sqrt{7+\sqrt{5}})$. Therefore $\sqrt{7+\sqrt{5}}$ is constructible.

(d) $(0.029)^{1/3} = \sqrt[3]{\frac{29}{1000}}$ is not constructible by the same argument as in (b).

(e) $22.5° = \frac{90°}{4}$. Since we can bisect an angle with ruler and compass, the angle $45° = \frac{90°}{2}$ is constructible and $22.5° = \frac{45°}{2}$ is also constructible. Intersecting the angle with the unit circle we can construct the point with coordinates $(\cos 22.5°, \sin 22.5°)$. Therefore $\tan 22.5° = \frac{\sin 22.5°}{\cos 22.5°}$ is also constructible.

9. Find all complex solutions of the equation $z^6 + z^3 + 1 = 0$.

Solution

Let $x = z^3$. Then x satisfies $x^2 + x + 1 = 0$ so $x = \frac{-1\pm\sqrt{-3}}{2} = \frac{-1\pm\sqrt{3}i}{2}$. We have two possibilities

1) $x = \frac{-1+\sqrt{3}i}{2} = \cos(2\pi/3) + i\sin(2\pi/3)$. Solving $z^3 = x = \cos(2\pi/3) + i\sin(2\pi/3)$ we get $z = \cos(2\pi/9 + \frac{2\pi k}{3}) + i\sin(2\pi/9 + \frac{2\pi k}{3})$ where $k = 0, 1, 2$. This gives 3 solutions
when $k = 0$ we get $z_1 = \cos(2\pi/9) + i\sin(2\pi/9)$
when $k = 1$ we get $z_2 = \cos(2\pi/9 + \frac{2\pi}{3}) + i\sin(2\pi/9 + \frac{2\pi}{3}) = \cos(\frac{8\pi}{9}) + i\sin(\frac{8\pi}{9})$
when $k = 2$ we get $z_3 = \cos(2\pi/9 + \frac{4\pi}{3}) + i\sin(2\pi/9 + \frac{4\pi}{3}) = \cos(\frac{14\pi}{9}) + i\sin(\frac{14\pi}{9})$

2) $x = \frac{-1-\sqrt{3}i}{2} = \cos(4\pi/3) + i\sin(4\pi/3)$. Solving $z^3 = x = \cos(4\pi/3) + i\sin(4\pi/3)$ we get $z = \cos(4\pi/9 + \frac{2\pi k}{3}) + i\sin(4\pi/9 + \frac{2\pi k}{3})$ where $k = 0, 1, 2$. As before, this gives 3 solutions
when $k = 0$ we get $z_4 = \cos(4\pi/9) + i\sin(4\pi/9)$
when $k = 1$ we get $z_5 = \cos(4\pi/9 + \frac{2\pi}{3}) + i\sin(4\pi/9 + \frac{2\pi}{3}) = \cos(\frac{10\pi}{9}) + i\sin(\frac{10\pi}{9})$
when $k = 2$ we get $z_6 = \cos(4\pi/9 + \frac{4\pi}{3}) + i\sin(4\pi/9 + \frac{4\pi}{3}) = \cos(\frac{16\pi}{9}) + i\sin(\frac{16\pi}{9})$

10. Let $p = 3, q = 11$ and $e = 7$. Let $N = 3 \cdot 11 = 33$. The receiver broadcasts the numbers $N = 33, e = 7$. The sender sends a secret message M to the receiver using RSA encryption. What is sent is the number $R = 6$.

    Decode to find the original message M.

    Solution

    We compute $\phi(N) = \phi(33) = (3-1)\cdot(11-1) = 20$. We need to find a natural number D such that $De \equiv 1(\mod \phi(N))$, i.e. such that $7D \equiv 1(\mod 20)$. This can be done Using Euclidean algorithm. We compute $20 = 2\cdot 7 + 6, 7 = 1 \cdot 6 + 1$ so that $1 = gcd(20, 7)$. Also, from $20 = 2 \cdot 7 + 6$ we can express 6 as $6 = 20 - 2 \cdot 7$. Plugging this into the second formula we get $1 = 7 - 6 = 7 - (20 - 2 \cdot 7) = 3 \cdot 7 - 20 \cdot 1$. Therefore we can take $D = 3$.

    To decode the message we need to compute $R^D(\mod N$, i.e. $6^3(\mod 33)$. We compute $6^3 = 216 = 6 \cdot 3 + 18$ and hence $M = 18$.

    Answer: $M = 18$.

11. Construct a polynomial with integer coefficients which has $\sqrt{2} + \sqrt{5}$ as a root.

    Solution

    Let $x = \sqrt{2} + \sqrt{5}$. Then it satisfies $x - \sqrt{2} = \sqrt{5}$. Squaring both sides we get $(x - \sqrt{2})^2 = (\sqrt{5})^2 = 5, x^2 - 2x\sqrt{2} + 2 = 5, x^2 - 3 = 2x\sqrt{2}$. Again squaring both sides we get $(x^2 - 3)^2 = (2x\sqrt{2})^2 = 8x^2, x^4 - 6x^2 + 9 = 8x^2, x^4 - 14x^2 + 9 = 0$.

    Answer: $\sqrt{2} + \sqrt{5}$ is a root of $x^4 - 14x^2 + 9 = 0$.