Solutions to Practice Final 3

1. The Fibonacci sequence is the sequence of numbers $F(1), F(2), \ldots$ defined by the following recurrence relations:
$F(1) = 1, F(2) = 1,\ F(n) = F(n-1) + F(n-2)$ for all $n > 2$.
For example, the first few Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, \ldots$

   (a) Prove by induction that for any $n \geq 1$ the consequtive Fibonacci numbers $F(n)$ and $F(n+1)$ are relatively prime.

   (b) Prove by induction that for any $n \geq 1$ the following identity holds

$$F(2) + F(4) + \ldots F(2n) = F(2n+1) - 1$$

Solution

(a) Since $F(1) = F(2) = 1$ the statement is true for $n = 1$.

Suppose we have proved that $gcd(F(n), F(n+1)) = 1$ for some $n \geq 1$. Observe that for any integers a and b we have that $d|a$ and $d|b$ if and only if $d|a$ and $d|a+b$. Therefore, $gcd(a, b) = gcd(a, a+b)$.

Using the above observation we conclude $gcd(F(n+1), F(n+2)) = gcd(F(n+1), F(n) + F(n+1)) = gcd(F(n+1), F(n)) = 1$ where the last equality holds by the induction assumption.

This proves the induction step and therefore $gcd(F(n), F(n+1)) = 1$ for any $n \geq 1$.

(b) First we check that the formula holds for $n = 1$:

$$F(2) = 1 = 2 - 1 = F(3) - 1$$

Induction step. Suppose we've already proved that

$$F(2) + F(4) + \ldots F(2n) = F(2n+1) - 1$$

for some $n \geq 1$. Then $F(2)+F(4)+\ldots F(2n)+F(2\cdot(n+1)) = F(2n+1)-1+F(2n+2) = F(2n+3) - 1 = F(2(n+1)+1) - 1$.

Therefore the formula holds for $n+1$. This proves the induction step and hence

$$F(2) + F(4) + \ldots F(2n) = F(2n+1) - 1$$

for any $n \geq 1$.

2. (a) Find the remainder when $7^{3^{100}}$ is divided by 20.

Solution

We find $\phi(20) = \phi(2^2 \cdot 5) = (2^2 - 2^1) \cdot (5 - 1) = 8$. Since $gcd(7, 20) = 1$ this implies that $7^8 \equiv 1 \pmod{20}$ by Euler's theorem. Thus we need to find $3^{100} \pmod{8}$. We have $3^2 = 9 \equiv 1 \pmod{8}$. Therefore $3^{100} = (3^2)^{50} \equiv 1^{50} \equiv 1 \pmod{8}$, i.e. $3^{100} = 8k + 1$ for some natural k. Hence $7^{3^{100}} = 7^{8k+1} = (7^8)^k \cdot 7 \equiv 1^k \cdot 7 \equiv 7 \pmod{20}$.

Answer: $7^{3^{100}} \equiv 7 \pmod{20}$.

(b) Find $2^{p!} (\mod p)$ where p is an odd prime.

Solution

By Fermat's theorem $2^{p-1} \equiv 1 \pmod{p}$. Since $p - 1$ divides $p!$ this implies that $2^{p!} \equiv 1 \pmod{p}$ too.

Answer: $2^{p!} \equiv 1 \pmod{p}$.

3. Prove that $q_1\sqrt{2} + q_2\sqrt{6}$ is irrational for any rational q_1, q_2 unless $q_1 = q_2 = 0$.

Solution

Suppose $x = q_1\sqrt{2} + q_2\sqrt{6}$ is rational and at least one of the numbers q_1, q_2 is not zero.

Case 1. $q_1 = 0, q_2 \neq 0$. This means that $x = q_2\sqrt{6}$ is rational and hence $\sqrt{6} = \frac{x}{q_2}$ is rational too. This is false and therefore this case is impossible.

Case 2. $q_1 \neq 0, q_2 = 0$. As above this means that $x = q_1\sqrt{2}$ is rational and hence $\sqrt{2} = \frac{x}{q_1}$ is also rational. This is known to be false and hence this case is impossible too.

Case 3. $q_1 \neq 0, q_2 \neq 0$. Squaring both sides of the formula $x = q_1\sqrt{2} + q_2\sqrt{6}$ we get $x^2 = 2q_1^2 + 6q_2^2 + 2q_1q_2\sqrt{12} = 2q_1^2 + 6q_2^2 + 4q_1q_2\sqrt{3}$. Therefore $\sqrt{3} = \frac{x^2 - 2q_1^2 - 6q_2^2}{4q_1q_2}$ is rational (note that the denominator in this fraction is not zero). This is a contradiction.

Thus, $q_1\sqrt{2} + q_2\sqrt{6}$ is irrational for any rational q_1, q_2 unless $q_1 = q_2 = 0$.

4. Suppose $(\phi(m), m) = 1$. Here m is a natural number and ϕ is the Euler function.

   Prove that $\sqrt{m}$ is irrational.

Solution

Let $m = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ be the prime decomposition of m where $p_1, \ldots, p_l$ are distinct primes. Then $\phi(m) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdot \ldots \cdot (p_l^{k_l} - p_l^{k_l - 1})$.

If some $k_i > 1$ this formula implies that p_i divides $\phi(m)$ and hence $gcd(\phi(m), m) \neq 1$. Thus, if $gcd(\phi(m), m) = 1$ then all k_i are equal to 1. Therefore $m = p_1 \cdot \ldots \cdot p_k$ is not a complete square and hence $\sqrt{m}$ is irrational.

5. Let $p = 11, q = 5$ and $E = 23$. Let $N = 11 \cdot 5 = 55$. The receiver broadcasts the numbers $N = 55, E = 23$. The sender sends a secret message M to the receiver using RSA encryption. What is sent is the number $R = 2$.

   Decode the original message M.

Solution

First we compute $\phi(N) = (5-1)\cdot(11-1) = 40$. Thus we need to find a decoder D such that $DE \equiv 1 \pmod{40}$ where $E = 23$. We find D using the Euclidean algorithm.

$40 = 23 \cdot 1 + 17, 17 = 40 \cdot 1 - 23 \cdot 1,$
$23 = 17 \cdot 1 + 6, 6 = 23 \cdot 1 - 17 \cdot 1 = 23 \cdot 1 - (40 \cdot 1 - 23 \cdot 1) = 23 \cdot 2 - 40 \cdot 1,$
$17 = 6 \cdot 2 + 5, 5 = 17 \cdot 1 - 6 \cdot 2 = (40 \cdot 1 - 23 \cdot 1) - (23 \cdot 2 - 40 \cdot 1) \cdot 2 = 40 \cdot 3 - 23 \cdot 5,$
$6 = 5 \cdot 1 + 1, 1 = 6 \cdot 1 - 5 \cdot 1 = (23 \cdot 2 - 40 \cdot 1) - (40 \cdot 3 - 23 \cdot 5) = 23 \cdot 7 - 40 \cdot 4.$

Thus $23 \cdot 7 \equiv 1 \pmod{40}$ and we can take $D = 7$.

Then $M = R^D \pmod{N} = 2^7 \pmod{55} = 128 \pmod{55} \equiv 18 \pmod{55}$.

Answer: $M = 18$.

6. (a) Find all complex roots of the equation

$$z^6 + (1-i)z^3 - i = 0$$

Solution

Put $y = z^3$. We first need to solve $y^2 + (1-i)y - i = 0$.
We have $y = \frac{-(1-i)\pm\sqrt{(1-i)^2+4i}}{2} = \frac{-(1-i)\pm\sqrt{1^2+i^2-2i-4i}}{2} = \frac{-(1-i)\pm\sqrt{1^2+i^2+2i}}{2} = \frac{-(1-i)\pm\sqrt{(1+i)^2}}{2}$
$= \frac{-(1-i)\pm(1+i)}{2}$ which gives $y_1 = \frac{-(1-i)+(1+i)}{2} = i$ and $y_2 = \frac{-(1-i)-(1+i)}{2} = -1$.
Next, we separately solve $z^3 = i$ and $z^3 = -1$.
From the first equation we get $z^3 = i = 1(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2})$ and hence $z = \sqrt[3]{1}((\cos\frac{\frac{\pi}{2}+2\pi k}{3} + i\sin\frac{\frac{\pi}{2}+2\pi k}{3}) = \cos(\frac{\pi}{6}+\frac{2\pi k}{3}) + i\sin(\frac{\pi}{6}+\frac{2\pi k}{3})$ for $k = 0, 1, 2$. Plugging in $k = 0, 1, 2$ this gives
$z_1 = \cos(\frac{\pi}{6}+0) + i\sin(\frac{\pi}{6}+0) = \frac{\sqrt{3}}{2} + \frac{i}{2},$
$z_2 = \cos(\frac{\pi}{6}+\frac{2\pi}{3}) + i\sin(\frac{\pi}{6}+\frac{2\pi}{3}) = \cos(\frac{5\pi}{6}) + i\sin(\frac{5\pi}{6}) = -\frac{\sqrt{3}}{2} + \frac{i}{2},$
$z_3 = \cos(\frac{\pi}{6}+\frac{4\pi}{3}) + i\sin(\frac{\pi}{6}+\frac{4\pi}{3}) = \cos(\frac{3\pi}{2}) + i\sin(\frac{3\pi}{2}) = -i.$
Similarly, from the second equation we get
$z^3 = -1 = \cos\pi + i\sin\pi$ and hence $z = \cos\frac{\pi+2\pi k}{3} + i\sin\frac{\pi+2\pi k}{3}$ for $k = 0, 1, 2$.
Plugging in $k = 0, 1, 2$ this gives
$z_4 = \cos\frac{\pi+0}{3} + i\sin\frac{\pi+0}{3} = \frac{\sqrt{3}}{2} + \frac{i}{2},$
$z_5 = \cos\frac{\pi+2\pi}{3} + i\sin\frac{\pi+2\pi}{3} = \cos\pi + i\sin\pi = -1,$
$z_6 = \cos\frac{\pi+4\pi}{3} + i\sin\frac{\pi+4\pi}{3} = \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} = \cos\frac{-\pi}{3} + i\sin\frac{-\pi}{3} = \frac{\sqrt{3}}{2} - \frac{i}{2}.$

(b) Express as $a + bi$ for some real a, b:

$$\frac{6^{100}}{(3+\sqrt{3}i)^{103}}$$

Solution

First we compute $|3+\sqrt{3}i| = \sqrt{9+3} = \sqrt{12} = 2\sqrt{3}$. Therefore, we can rewrite $3+\sqrt{3}i = 2\sqrt{3}(\frac{\sqrt{3}}{2}+\frac{i}{2}) = 2\sqrt{3}(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6})$.
Thus,

$$\frac{6^{100}}{(3+\sqrt{3}i)^{103}} = \frac{6^{100}}{(2\sqrt{3}(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}))^{103}} = \frac{6^{100}}{(2\sqrt{3})^{103}}\cdot(\cos(-\frac{\pi}{6})+i\sin(-\frac{\pi}{6}))^{103}$$

$$= \frac{6^{100}}{(2\sqrt{3})^{103}}\cdot(\cos(-\frac{103\pi}{6})+i\sin(-\frac{103\pi}{6})) = \frac{6^{100}}{(2\sqrt{3})^{103}}\cdot(\cos(-17\pi-\pi/6)+i\sin(-17\pi-\pi/6))$$

$$= \frac{6^{100}}{(2\sqrt{3})^{103}}\cdot(\cos(5\pi/6)+i\sin(5\pi/6)) = \frac{6^{100}}{(2\sqrt{3})^{103}}\cdot(-\frac{\sqrt{3}}{2}+\frac{i}{2})$$

7. A complex number is called *algebraic* if it is a root of a polynomial with integer coefficients.

   Prove that the set of algebraic numbers is countable.

Solution

For a polynomial f let us denote by Z_f the set of roots of f. Then the set of algebraic numbers A is equal to $\bigcup_{f\in P} Z_f$ where P is the set of all nonzero polynomials. Since a nonzero polynomial of degree n has at most n roots we have that Z_f is finite (and hence countable) for every f. Since a union of countably many countable sets is countable it's therefore enough to prove that P is countable. We can write P as the union $P = \bigcup_{n\in N} P_n$ where P_n is the set of nonzero polynomials of degree n. A polynomial $f(x)$ of degree n is given by $f(x) = a_n x^n + \ldots + a_1 x + a_0$. The correspondence $f \mapsto (a_n, a_{n-1}, \ldots, a_1, a_0)$ give an injective map $P_n \to Z^{n+1}$ and since $|Z^{n+1}| = |N^{n+1}| = |N|$ we conclude that P_n is countable. Therefore $P = \bigcup_{n\in N} P_n$ is also countable as a union of countably many countable sets and hence so is A.

8. Suppose $0 < \alpha < \pi/2$ satisfies $\cos\alpha = \frac{1}{6}$. Prove that the angle α can not be trisected with a ruler and a compass.

Solution

Recall that $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ for any θ.

Note that the angle α is constructible since $\cos\alpha = \frac{1}{6}$ is a constructible number.

Suppose α can be trisected. Then $x = \cos(\alpha/3)$ is also constructible and satisfies $4x^3 - 3x = \frac{1}{6}$ or $8x^3 - 6x = \frac{1}{3}, (2x)^3 - 3\cdot(2x) = \frac{1}{3}$. If x is constructible then so is $y = 2x$ which satisfies $y^3 - 3y = \frac{1}{3}, 3y^3 - 9y - 1 = 0$. This is a cubic polynomial with rational coefficients. If it has a constructible root it also has a rational one. Suppose $\frac{p}{q}$ is a rational root where $gcd(p,q) = 1$. By the rational root theorem we must have that $p|-1$ and $q|3$. Therefore, $p = \pm 1, q = \pm 1, \pm 3$ and $\frac{p}{q} = \pm 1, \pm\frac{1}{3}$. Plugging in these numbers into $3y^3 - 9y - 1 = 0$ we get

$3\cdot 1^3 - 9 - 1 = -7 \neq 0, 3\cdot(-1)^3 - 9\cdot(-1) - 1 = 5 \neq 0$, $3\cdot(\frac{1}{3})^3 - 9\cdot\frac{1}{3} - 1 = \frac{1}{9} - 4 \neq 0$, $3\cdot(-\frac{1}{3})^3 - 9\cdot(-\frac{1}{3}) - 1 = -\frac{1}{9} + 2 \neq 0$.

Thus $3y^3 - 9y - 1 = 0$ has no rational roots. This is a contradiction and hence α can not be trisected with a ruler and a compass.

9. Let S be that set of all functions $f\colon \mathbb{R} \to \mathbb{R}$.

   Prove that $|S| > |\mathbb{R}|$.

Solution

The set S contains the set $T = \{f\colon \mathbb{R} \to \{0,1\}\}$. Therefore $|S| \geq |T|$. However T is bijective to $P(\mathbb{R})$ which is the set of all subsets of $\mathbb{R}$ and $|P(\mathbb{R})| > |\mathbb{R}|$ by Cantor's theorem.

Therefore $|S| \geq |T| = |P(\mathbb{R})| > |\mathbb{R}|$.

10. For each of the following answer "true" or "false". Justify your answer.

   a) $\sqrt{\frac{\sqrt{5}}{\sqrt[3]{2}+\sqrt{11}}}$ is constructible.

Solution

Suppose $x = \sqrt{\frac{\sqrt{5}}{\sqrt[3]{2}+\sqrt{11}}}$ is constructible. Then $x^2 = \frac{\sqrt{5}}{\sqrt[3]{2}+\sqrt{11}}$ is also constructible and hence so is $\frac{1}{x^2} = \frac{\sqrt[3]{2}+\sqrt{11}}{\sqrt{5}}$. Since both $\sqrt{5}$ and $\sqrt{11}$ are constructible this implies that $\sqrt[3]{2}$ is constructible too. But $\sqrt[3]{2}$ is a root of the cubic polynomial with rational coefficients $y^3 - 2 = 0$. If it has a constructible root it also has a rational one. Suppose $\frac{p}{q}$ is a rational root where $gcd(p,q) = 1$. By the rational root theorem we must have that $p|-2$ and $q|1$ so that $p = \pm 1, \pm 2, q = \pm 1$ and therefore $p/q = \pm 1, \pm 2$. Plugging these numbers into $y^3 - 2 = 0$ we see that none are roots.

$1^3 - 2 = -1 \neq 0, (-1)^3 - 2 = -3 \neq 0, 2^3 - 2 = 6 \neq 0, (-2)^3 - 2 = -10 \neq 0$.

Therefore $\sqrt[3]{2}$ is not constructible which mans that $\sqrt{\frac{\sqrt{5}}{\sqrt[3]{2}+\sqrt{11}}}$ is not constructible either.

Answer: False.

b) If x is not constructible then $\sqrt{x}$ is also not constructible.

Solution

If $\sqrt{x}$ is constructible then $x = \sqrt{x} \cdot \sqrt{x}$ is constructible too because the product of two constructible numbers is constructible.

Answer: True.

c) If x is constructible then $\sqrt[8]{x}$ is also constructible.

Solution

Square root of a constructible number is constructible. Therefore if x is constructible then so are $\sqrt{x}$, $\sqrt{\sqrt{x}} = \sqrt[4]{x}$ and $\sqrt{\sqrt[4]{x}} = \sqrt[8]{x}$.

Answer: True.