(1) (10 pts) The pigeonhole principle states that if $n$ items are put into $m$ pigeonholes with $n > m$, then at least one pigeonhole must contain more than one item.

Prove the pigeonhole principle by induction in $m$.

**Solution**

We prove it by induction on $m$.

If $m = 1$ then the statement is obvious as we have $n > 1$ objects and only one pigeonhole.

Induction step. Suppose the pigeonhole principle has been proved for $m - 1 \geq 1$ and we want to prove it for $m$.

Suppose we have $n > m$ items distributed between $m$ pigeonholes. Consider the last pigeonhole. If it contains more than one item we are done. Suppose it has exactly one item. Then the remaining $n - 1$ items are distributed between the first $m - 1$ pigeonholes and since $n - 1 > m - 1$, by the induction assumption we can conclude that one of the first $m - 1$ holes contains at least two items.

Similarly, if the last pigeonhole is empty and contains no items at all then we have that $n$ items are distributed between the first $m - 1$ pigeonholes. Since $n > m > m - 1$, we can again use the induction assumption to conclude that one of the first $m - 1$ holes contains at least two items.

(2) (15 pts) Let $a, b$ be relatively prime natural numbers bigger than 1.

Prove that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

**Hint:** Use that $gcd(a, b)$ can be written as $gcd(a, b) = ax + by$ for some integer $x$ and $y$.

**Solution 1 (not using the hint)**

Since $(a, b) = 1$, by Euler’s theorem $a|(b^{\phi(a)} - 1)$ and therefore

$$a|(a^{\phi(b)} + (b^{\phi(a)} - 1)) = a^{\phi(b)} + b^{\phi(a)} - 1$$
Similarly $b | (a^{\phi(b)} - 1)$ and hence 

$$b | (b^{\phi(a)} + (a^{\phi(b)} - 1)) = a^{\phi(b)} + b^{\phi(a)} - 1$$

Since $(a, b) = 1$ this implies that $ab | (a^{\phi(b)} + b^{\phi(a)} - 1)$ i.e. $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$

**Solution 2 (using the hint)**

Since $\gcd(a, b) = 1$ there exist integer $x$ and $y$ such that $ax + by = 1$.

By Euler’s theorem $a^{\phi(b)} \equiv 1 \pmod{b}$. Therefore, $a^{\phi(b)} \equiv 1 - kb \pmod{b}$ for any integer $k$. In particular, $a^{\phi(b)} \equiv 1 -yb \pmod{b}$. But $1 - yb = xa \equiv 0 \pmod{a}$

Therefore $a^{\phi(b)} - (1 - yb) = a^{\phi(b)} - ax \equiv 0 \pmod{a}$. Thus, $a | a^{\phi(b)} - (1 - yb)$ and $b | a^{\phi(b)} - (1 - yb)$ and hence $ab | a^{\phi(b)} - (1 - yb)$ since $\gcd(a, b) = 1$. In other words, $a^{\phi(b)} \equiv 1 - yb \pmod{ab}$.

Similarly, $b^{\phi(a)} \equiv 1 - xa \pmod{ab}$. Adding these congruencies we obtain 

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 - yb + 1 - xa = 2 - (ax + by) = 1 \pmod{ab}$$

(3) (10 pts) Let $n \geq 2$ be a composite number.

Prove that there exists a prime number $p \leq \sqrt{n}$ which divides $n$.

**Solution**

A composite number contains at least two prime factors. Therefore $n = pqc$ where $p, q$ are prime and $c \geq 1$. We can assume that $p \leq q$ (otherwise we can just rename them).

Therefore $n = pqc \geq pq \geq p^2$ and hence $\sqrt{n} \geq p$.

(4) (a) (20 pts) Let $p > 1$ be a prime number.

Find $2^{(p!)^2} \pmod{p}$.

**Solution**

If $p = 2$ then $2^{(p!)^2} \equiv 0 \pmod{2}$.

Suppose $p > 2$. Then $p$ is not divisible by 2 and hence $2^{p-1} \equiv 1 \pmod{p}$ by Fermat’s theorem. Therefore $2^{k(p-1)} = (2^{p-1})^k \equiv 1 \pmod{p}$ for any natural $k$.

Since $(p!)^2$ is divisible by $p - 1$ this implies that $2^{(p!)^2} \equiv 1 \pmod{p}$.

(b) Find $(26!)^{143} \pmod{29}$.

**Solution**

Recall that by Wilson’s theorem $(p - 1)! \equiv -1 \pmod{p}$ for any prime $p$.

Applying this to $p = 29$ we see that $28! \equiv -1 \pmod{29}$.

We can rewrite
28! = 26! · 27 · 28. Since 27 \equiv -2 \pmod{29} and 28 \equiv -1 \pmod{29} this gives 26! · (-2) · (-1) \equiv -1 \pmod{29} or 26! · (-2) \equiv 1 \pmod{29}.

Therefore

\[(26!)^{143} \cdot (-2)^{143} \equiv 1 \pmod{29}\]

Let’s find (-2)^{143} \pmod{29}. By Fermat’s theorem (-2)^{28} \equiv 1 \pmod{29}. Since 143 = 5 \cdot 28 + 3 this gives (-2)^{143} \equiv (-2)^3 = -8 \pmod{29}.

Thus (26!)^{143} \cdot (-8) \equiv 1 \pmod{29}. Therefore we need to solve the equation -8x \equiv 1 \pmod{29}. Since (8, 29) = 1 it has only one solution mod 29. We can find it using the Euclidean algorithm or by guessing. Observe that 8 \cdot 11 = 88 = 3 \cdot 29 + 1. Hence (-11) \cdot (-8) \equiv 1 \pmod{29}.

Therefore, (26!)^{143} \equiv -11 \equiv 18 \pmod{29}.

**Answer:** (26!)^{143} \equiv 18 \pmod{29}.

(c) Find 2^{3^{101}} \pmod{15}.

\[\text{Solution}\]

Observe that (2, 15) = 1. We compute \(\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4 = 8.\) Therefore, by Euler’s theorem, \(2^{\phi(15)} = 2^8 \equiv 1 \pmod{15}.\)

Thus we need to find 3^{101} \pmod{8}. Notice that 3^2 = 9 \equiv 1 \pmod{8}. Hence 3^{2k} \equiv 1 \pmod{8} for any natural k. Therefore, 3^{100} = 3^{100} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{8}. In other words, 3^{101} = 3 + 8m for some natural number m.

Therefore \(2^{3^{101}} = 2^{3+8m} \equiv 2^3 = 8 \pmod{15}.\)

**Answer:** \(2^{3^{101}} \equiv 8 \pmod{15}.\)

(5) (10 pts) Let n be a natural number. Prove that \(\sqrt[10]{n}\) is rational if and only if \(n\) is a complete 10th power, i.e. \(n = m^{10}\) for some natural number m.

\[\text{Solution}\]

If \(n = m^{10}\) is a complete 10th power then, obviously, \(\sqrt[10]{n} = m\) is rational.

Conversely, suppose \(\sqrt[10]{n}\) is rational. Then \(\sqrt[10]{n} = \frac{p}{q}\) for some integer \(p, q\) and by reducing the fraction if necessary we can assume that \(gcd(p, q) = 1.\)

Then \(\frac{p}{q}\) is a rational solution of the equation \(x^{10} - m = 0.\) Since \(gcd(p, q) = 1,\) by the Rational Root Theorem this implies that \(p|n\) and \(q|1.\) Therefore, \(q = \pm 1\) and hence \(\frac{p}{q} = m\) is actually an integer. This means that \(n = (\frac{p}{q})^{10} = m^{10}\) is a complete 10th power.
(6) (15 pts) Let $p = 11, q = 3$ and $E = 13$. Let $N = 11 \cdot 3 = 33$. The receiver broadcasts the numbers $N = 33, E = 13$. The sender wants to send a secret message $M$ to the receiver using RSA encryption. What is sent is the number $R = 2$.

Decode the original message $M$.

Solution

We compute $\phi(N) = \phi(3 \cdot 11) = 2 \cdot 10 = 20$. To decode the message we need to find $D$ such that $ED \equiv 1 \pmod{\phi(N)}$ which in our case means $13D \equiv 1 \pmod{20}$. Observe that $13 \cdot 3 = 39 \equiv -1 \pmod{20}$. Therefore, $13 \cdot (-3) \equiv 1 \pmod{20}$ and $13 \cdot 17 \equiv 1 \pmod{20}$. Thus we can take $D = 17$. This can also be computed using the Euclidean algorithm.

$20 = 13 \cdot 1 + 7, 13 = 7 \cdot 1 + 6, 7 = 6 \cdot 1 + 1, 6 = 1 \cdot 6 + 0$. Thus $1 = gcd(13, 20)$.

From the first equation we get $7 = 20 \cdot 1 - 13 \cdot 1$. From the second that $6 = 13 \cdot 1 - 7 \cdot 1 = 13 \cdot 1 - (20 \cdot 1 - 13 \cdot 1) \cdot 1 = 13 \cdot 2 - 20 \cdot 1$. Next, $1 = 7 \cdot 1 - 6 \cdot 1 = (20 \cdot 1 - 13 \cdot 1) \cdot 1 - (13 \cdot 2 - 20 \cdot 1) \cdot 1 = 20 \cdot 2 - 13 \cdot 3$.

Thus $20 \cdot 2 - 13 \cdot 3 = 1$ which means that $13 \cdot (-3) \equiv 1 \pmod{20}$ and hence $13 \cdot 17 \equiv 1 \pmod{20}$.

Either way we can take $D = 17$.

By the general RSA procedure, $M = R^D \pmod{N}$. In our case this gives $M = 2^{17} \pmod{33}$. To compute it notice that $2^5 = 32 \equiv -1 \pmod{33}$. Therefore, $2^{17} = (2^5)^3 \cdot 2^2 \equiv (-1)^3 \cdot 4 \equiv -4 \equiv 29 \pmod{33}$.

Answer: $M = 29$. 