Solutions to Exam 1

Problem 1. a) State Fermat's Little Theorem and Euler's Theorem.

b) Let m, n be relatively prime positive integers. Prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn} .$$

Solution: a)

Fermat's Little Theorem: Let p be a prime. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

for any integer a not divisible by p.

Euler's Theorem: Let n be a positive integer. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for any integer a relatively prime to n.

b) By Euler's Theorem, $m^{\phi(n)} \equiv 1 \pmod{n}$. Clearly $n^{\phi(n)} \equiv 0 \pmod{n}$. Thus

$$m^{\phi(n)} + n^{\phi(n)} \equiv 1 \pmod{n} .$$

Similarly, $n^{\phi(m)} \equiv 1 \pmod{m}$ and $m^{\phi(m)} \equiv 0 \pmod{m}$ so

$$m^{\phi(n)} + n^{\phi(n)} \equiv 1 \pmod{m} .$$

In other words, $m^{\phi(n)} + n^{\phi(n)} - 1$ is divisible by both m and n. Since m and n are relatively prime, we conclude that $m^{\phi(n)} + n^{\phi(n)} - 1$ is divisible by mn, i.e. $m^{\phi(n)} + n^{\phi(n)} \equiv 1 \pmod{mn}$.

Problem 2. a) State Chinese Remainder Theorem.

b) Find all positive integers smaller than 200 which leave remainder $1, 3, 4$ upon division by $3, 5, 7$ respectively.

Solution: a)

Chinese Remainder Theorem: Let $n_1, ..., n_k$ be pairwise relatively prime positive integers and let $N = n_1 \cdot n_2 \cdot ... \cdot n_k$. Given integers $a_1, ..., a_k$ there is integer x such that

$x \equiv a_i \pmod{n_i}$ for $i = 1, 2, ..., k$. Moreover, an integer y satisfies the congruences iff $N|(x-y)$ (so all integers satisfying the congruences are given by $x+mN$, $m \in \mathbb{Z}$).

b) The problem asks us to find all integers x such that $0 < x < 200$ and

$$x \equiv 1 \pmod{3}\ ,\ x \equiv 3 \pmod{5}\ ,\ x \equiv 4 \pmod{7}\ .$$

In order to find a solution to these congruences, we observe that

$$12 \cdot 3 + (-1) \cdot 35 = 1,$$

$$(-4) \cdot 5 + 21 = 1,$$

$$(-2) \cdot 7 + 15 = 1.$$

Thus a solution is given by $x = (-35)+3\cdot 21+4\cdot 15 = 88$. It follows that all solutions are given by the formula $x = 88 + 105m$, $m \in Z$. We get a positive solution smaller than 200 only for $m = 0, 1$, so 88 and 193 are the only solutions to our problem.

Problem 3. a) Define $\gcd(a, b)$. Using Euclid's algorithm compute $\gcd(889, 168)$ and find $x, y \in \mathbb{Z}$ such that $\gcd(889, 168) = x \cdot 889 + y \cdot 168$ (check your answer).

b) Let a be an integer. Prove that $\gcd(3a + 5, 7a + 12) = 1$. **Hint:** If $d|u$ and $d|w$ then $d|su + tw$ for any integers s, t.

Solution: a) $\gcd(a, b)$ is the largest positive integer which divides both a and b. It is the unique positive integer d with the property that $\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(d)$.

We have

$$889 = 5 \cdot 168 + 49,$$

$$168 = 3 \cdot 49 + 21,$$

$$49 = 2 \cdot 21 + 7,$$

$$21 = 3 \cdot 7 + 0.$$

By Euclid's algorithm, $\gcd(889, 168) = 7$. Furthermore,

$$7 = 49-2\cdot 21 = 49-2\cdot(168-3\cdot 49) = 7\cdot 49-2\cdot 168 = 7\cdot(889-5\cdot 168)-2\cdot 168 = 7\cdot 889-37\cdot 168.$$

Thus $x = 7$, $y = -37$ works.

b) Note that $3(7a + 12) + (-7)(3a + 5) = 1$. Thus any common divisor of $3a + 5$ and $7a + 12$ must divide 1. It follows that $\gcd(3a + 5, 7a + 12) = 1$.

Problem 4. a) Define prime numbers. State the Fundamental Theorem of Arithmetic. Explain the notation: $p^k||m$.

b) Let $n = p_1^{a_1}p_2^{a_2}...p_s^{a_s}$, where $p_1 < p_2 < ... < p_s$ are prime numbers. Prove that n is a perfect square (i.e. $n = m^2$ for some integer m) iff $a_1, a_2, ..., a_s$ are all even.

c) Suppose that $k \cdot l$ is a perfect square and $\gcd(k, l) = 1$. Prove that both k and l are perfect squares.

Solution: a) A **prime number** is any integer $p > 1$ such that $\text{div}(p) = \{1, p\}$. **Fundamental Theorem of Arithmetic:** Any positive integer $n > 1$ can be factored in unique way as $n = p_1^{a_1}p_2^{a_2}...p_s^{a_s}$, where $p_1 < p_2 < ... < p_s$ are prime numbers and $a_1, ..., a_s$ are positive integers.

The notation $p^k||m$ means that k is the highest power of p which divides m, i.e. $p^k|m$ but $p^{k+1} \nmid m$ (or, equivalently, k is the exponent with which p appears in the prime factorization of m).

b) Suppose that $n = m^2$ is a perfect square. If $m = q_1^{b_1}q_2^{b_2}...q_t^{b_t}$ is a prime factorization of m then $m^2 = q_1^{2b_1}q_2^{2b_2}...q_t^{2b_t}$ is a prime factorization of $n = m^2$. By uniqueness of factorization, we have $s = t$, $q_i = p_i$ and $a_i = 2b_i$ for $i = 1, 2, ..., s$. In particular, all a_i's are even.

Conversely, if all a_i's are even then $m = p_1^{a_1/2}p_2^{a_2/2}...p_s^{a_s/2}$ is n integer and $n = m^2$ so n is a perfect square.

c) Let $n = kl$ be a perfect square. Suppose that k is not a perfect square. Then, by b), there is a prime divisor p of k such that $p^a||k$ and a is odd. Since p cannot divide l, we have $p^a||n$. This however contradicts b), since n is a perfect square (so for any prime q we have $q^b||n$ for some <u>even</u> b).

Problem 5. a) Define quadratic residues and non-residues modulo a prime p. Find all quadratic residues modulo 11.

b) Suppose that $n = a^2 + b^2$ for some integers a, b. Prove that $n \not\equiv 3 \pmod 4$.

Solution: a) An integer a is called a **quadratic residue** modulo a prime p if $p \nmid a$ and $a \equiv x^2 \pmod p$ for some integer x. An integer a is called a **quadratic non-residue** modulo a prime p if there is no integer x such that $a \equiv x^2 \pmod p$.

We know that a is a quadratic residue modulo p iff $a \equiv i^2 \pmod{p}$ for some $i \in \{1, 2, .., (p-1)/2\}$. Since $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 \equiv 5 \pmod{11}$, $5^2 = 25 \equiv 3 \pmod{11}$, an integer a is a quadratic residue modulo 11 iff a is congruent modulo 11 to one of $1, 3, 4, 5, 9$.

b) Note that for any integer m we have either $m^2 \equiv 0 \pmod{4}$ or $m^2 \equiv 1 \pmod{4}$ (in fact, m is congruent to one of $0, 1, 2, 3$ modulo 4 and $0^2 \equiv 2^2 \equiv 0 \pmod{4}$, $1^2 \equiv 3^2 \equiv 1 \pmod{4}$). Thus both $a^2 \equiv 0, 1 \pmod{4}$, $b^2 \equiv 0, 1 \pmod{4}$. Thus $n = a^2 + b^2 \equiv 0, 1, 2 \pmod{4}$, i.e. $n \not\equiv 3 \pmod{4}$.

Problem 6. Prove that $n^{21} \equiv n \pmod{30}$ for every integer n.

Solution: Let us note that if p is a prime then $n^{k(p-1)+1} \equiv n \pmod{p}$ for any integer n and any $k > 0$. In fact, if $p|n$ then both sides are $\equiv 0 \pmod{p}$ and if $p \nmid n$ then Femrat's Little Theorem tells us that $n^{p-1} \equiv 1 \pmod{p}$ so

$$n^{k(p-1)+1} = (n^{p-1})^k \cdot n \equiv n \pmod{p} .$$

We apply this observation to $p = 2, 3, 5$. Since $21 = 20 \cdot (2-1)+1 = 10 \cdot (3-1)+1 = 5 \cdot (5-1)+1$, we have

$$n^{21} \equiv n \pmod{2} , \ n^{21} \equiv n \pmod{3} , \ n^{21} \equiv n \pmod{5} .$$

In other words, $n^{21} - n$ is divisible by 2, 3 and 5 and since these numbers are pairwise relatively prime, $n^{21} - n$ is divisible by their product $2 \cdot 3 \cdot 5 = 30$, i.e. $n^{21} \equiv n \pmod{30}$

Problem 7. Let $a > 1$, $n > 1$ be integers.

a) What is the order of a modulo $a^n + 1$?

b) Prove that $2n|\phi(a^n + 1)$.

Solution: Recall that if $\gcd(a, m) = 1$ then $\mathrm{ord}_m(a)$ is the smallest positive integer s such that $a^s \equiv 1 \pmod{m}$. We have $a^k \equiv 1 \pmod{m}$ iff $\mathrm{ord}_m(a)|k$.

a) Clearly $\gcd(a, a^n + 1) = 1$ (any divisor of a is a divisor of a^n). Let $s = \mathrm{ord}_{a^n+1}(a)$ be the order of a modulo $a^n + 1$. Note that $s > n$ since $1 \leq a^i < a^n + 1$ for $0 < i \leq n$. Since $a^n \equiv -1 \pmod{a^n + 1}$, we have $a^{2n} \equiv 1 \pmod{a^n + 1}$. Thus $s|2n$. The only divisor of $2n$ greater than n is $2n$ itself, so $s = 2n$.

b) By Euler's Theorem, we have $a^{\phi(a^n+1)} \equiv 1 \pmod{a^n+1}$. Thus

$$\mathrm{ord}_{a^n+1}(a) | \phi(a^n+1).$$

Since $\mathrm{ord}_{a^n+1}(a) = 2n$ by a), we see that $2n | \phi(a^n+1)$.