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

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

c) Find the remainder of 31^{2008} upon division by 36.

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

c) Note that $(31, 36) = 1$. Thus $31^{\phi(36)} \equiv 1 \pmod{36}$ by Euler's Theorem. Now $36 = 2^2 \cdot 3^2$, so $\phi(36) = 2 \cdot 3 \cdot 3 = 12$. Therefore $31^{12} \equiv 1 \pmod{36}$. Observe that $2008 = 12 \cdot 167 + 4$, so

$$31^{2008} = (31^{12})^{167} \cdot 3^4 \equiv 31^4 \pmod{36} .$$

Thus it suffices to find the remainder of 31^4 upon division by 36. Since $31 \equiv -5 \pmod{36}$, we have $31^2 \equiv (-5)2 = 25 \equiv -11 \pmod{36}$, and $31^4 \equiv (-11)^2 = 121 \equiv 13 \pmod{36}$. The reminder in question is therefore equal to 13.

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. Show your work.

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 any integers $a_1, ..., a_k$, the system of congruences $x \equiv a_i \pmod{n_i}$, $i = 1, 2, ..., k$, has unique solution x such that $0 \leq x < N$. Moreover, an integer y satisfies these 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 follow the algorithm. We have $N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$.

We solve $N_1 x_1 \equiv 1 \pmod{3}$, i.e. $2x_1 \equiv 1 \pmod{3}$, which has a solution $x_1 = 2$.

Next we solve $N_2 x_2 \equiv 3 \pmod{5}$, i.e. $x_2 \equiv 3 \pmod{5}$, which has a solution $x_2 = 3$.

Finally, we solve $N_3 x_3 \equiv 4 \pmod{7}$, i.e. $x_3 \equiv 4 \pmod{7}$, which has a solution $x_3 = 4$.

A solution is given by $x = N_1 x_1 + N_2 x_2 + N_3 x_3 = 70 + 63 + 60 = 193$. The smallest positive solution is then $193 - 105 = 88$ and 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 (a, b). Using Euclid's algorithm compute $(889, 168)$ and find $x, y \in \mathbb{Z}$ such that $(889, 168) = x \cdot 889 + y \cdot 168$ (check your answer!).

b) Let a be an integer. Prove that $(3a + 5, 7a + 12) = 1$. **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 called the greatest common divisor of a and b.

Euclid's algorithm yields:

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

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

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

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

It follows that $\gcd(889, 168) = 7$. Working backwards,

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

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

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. Solve the following congruences

a) $18x \equiv 12 \pmod{28}$ b) $3x^2 + 2x - 4 \equiv 0 \pmod{17}$

Solution: a) Using Euclid's algorithm we find that $(18, 28) = 2$. Thus the congruence $18x \equiv 12 \pmod{28}$ has two solutions modulo 28, given by $x \equiv x_0 \pmod{28}$ or $x \equiv x_0 + 14 \pmod{28}$, where x_0 is any particular solution. To find a particular solution, we work the Euclid's algorithm backwards to get $2 = 2 \cdot 28 + (-3) \cdot 18$. Multiplying by 6, we see that $12 = 12 \cdot 28 - 18 \cdot 18 \equiv 18 \cdot (-18) \pmod{28}$. Thus $x_0 = -18$ is a particular solution so the solutions are $x \equiv -18 \pmod{28}$ or $x \equiv -4 \pmod{28}$, which can be written as $x \equiv 10 \pmod{28}$ or $x \equiv 24 \pmod{28}$.

b) Note that $3 \cdot 6 = 18 \equiv 1 \pmod{17}$, i.e. 6 is the inverse of 3 modulo 17. We multiply our congruence by 6 and get $18x^2 + 12x - 24 \equiv 0 \pmod{17}$, i.e. $x^2 + 12x - 7 \equiv 0 \pmod{17}$. Now we complete to squares:

$$x^2 + 12x - 7 = (x + 6)^2 - 36 - 7 \equiv (x + 6)^2 - 9 \pmod{17}.$$

Thus $(x + 6)^2 \equiv 9 = 3^2 \pmod{17}$ and therefore $x + 6 \equiv 3 \pmod{17}$ or $x + 6 \equiv -3 \pmod{17}$. Equivalently, $x \equiv -3 \equiv 14 \pmod{17}$ or $x \equiv -9 \equiv 8 \pmod{17}$.

Problem 5. a) Define the Legendre symbol $\left(\frac{a}{p}\right)$ (state clearly all assumptions) and state its properties.

b) Is 91 a quadratic residue modulo 127? Justify your answer.

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 $a \equiv x^2 \pmod{p}$. When p is an odd prime and $p \nmid a$ then we define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p; \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Legendre symbol has the following properties.

1. If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$ for any integer a relatively prime to p.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any integers a, b relatively prime to p.
4. Euler's Criterion: $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
5. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}; \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$ and $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}; \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$
6. Qadratic Reciprocity: If p and q are distinct odd prime numbers then
$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \equiv q \pmod{4}; \\ \left(\frac{p}{q}\right) & \text{if at least one of } p, q \text{ is } \equiv 1 \pmod{4}. \end{cases}$$

b) Note that $91 \equiv -36 \pmod{127}$. Thus, by properties 1,2,5 we have

$$\left(\frac{91}{127}\right) = \left(\frac{-36}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{36}{127}\right) = \left(\frac{-1}{127}\right) = -1.$$

Thus 91 is not a quadratic residue modulo 127.

Second method. Note that $91 = 7 \cdot 13$. We use the quadratic reciprocity:

$$\left(\frac{91}{127}\right) = \left(\frac{7}{127}\right)\left(\frac{13}{127}\right) = -\left(\frac{127}{7}\right)\left(\frac{127}{13}\right) = -\left(\frac{1}{7}\right)\left(\frac{10}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) =$$

$$= \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Thus 91 is not a quadratic residue modulo 127.

Problem 6. a) Define a primitive root modulo m. Prove that 2 is a primitive root modulo 25.

b) Show that if $(a, 77) = 1$ then 77 divides $a^{30} - 1$.

c) Is there a primitive root modulo 77? Explain your answer.

Solution: a) A primitive root modulo m is any integer a such that $\mathrm{ord}_m a = \phi(m)$. In other words, a is a primitive root modulo m if $a^{\phi(m)} \equiv 1 \pmod{m}$ and $a^k \not\equiv 1 \pmod{m}$ for $1 \leq k < \phi(m)$.

We have $\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$. Thus, the order of 2 modulo 25 is a divisor of 20, so it can be $1, 2, 4, 5, 10$ or 20. By inspection, we check that 20 is the smallest among these exponents which works. Thus the order of 2 modulo 25 is equal to 20 and therefore 2 is a primitive root modulo 25.

b) Note that $77 = 7 \cdot 11$. If $(a, 77) = 1$ then $(a, 7) = 1 = (a, 11)$. Thus, by Fermat's Little Theorem, we have $a^6 \equiv 1 \pmod{7}$ and $a^{10} \equiv 1 \pmod{11}$. Raising both sides of the first congruence to the power 5 and both sides of the second to the power 3 we get $a^{30} \equiv 1 \pmod{7}$ and $a^{30} \equiv 1 \pmod{11}$. Since $(7, 11) = 1$, we conclude that $a^{30} \equiv 1 \pmod{77}$.

c) Note that $\phi(77) = \phi(7 \cdot 11) = 6 \cdot 10 = 60$. If a were a primitive root modulo 77 then $\mathrm{ord}_{77} a = 60$. However, we know by part b) that $a^{30} \equiv 1 \pmod{77}$, so $\mathrm{ord}_{77} a | 30$ and therefore the order cannot be 60. This proves that there does not exist a primitive root modulo 77.

Problem 7. 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 8. Let p be a prime such that $p \equiv 2 \pmod 3$. Prove that the equation $x^3 \equiv a \pmod p$ is solvable for every integer a.

Solution: Let g be a primitive root modulo p. If $p|a$ then $x = 0$ is a solution. If $(a, p) = 1$ then $a \equiv g^k \pmod p$ for some k. We would like to find $m > 0$ such that $g^k \equiv g^{3m} \pmod p$. Then $x = g^m$ is a solution. Since the order of g modulo p is $p - 1$, we have $g^k \equiv g^{3m} \pmod p$ iff $(p-1)|(k-3m)$, i.e. $k \equiv 3m \pmod{p-1}$. Since $p \equiv 2 \pmod 3$, we have $(p-1, 3) = 1$ and therefore for any k there is an m such that $k \equiv 3m \pmod{p-1}$. Clerly we can choose such m positive, and then $x = g^m$ is a solution.

Problem 9. Let p be an odd prime such that $p|a^2 + b^2$ for some integers a, b relatively prime to p. Prove that $p \equiv 1 \pmod 4$

Solution: We have $a^2 \equiv -b^2 \pmod p$. Raising both sides to the power $(p-1)/2$ we get

$$a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p \ .$$

Since $a^{p-1} \equiv 1 \equiv b^{p-1} \pmod p$ by Fermat's Little Theorem, we see that $1 \equiv (-1)^{(p-1)/2} \pmod p$. This implies that $1 = (-1)^{(p-1)/2}$, which holds if and only if $p \equiv 1 \pmod 4$.

Second solution: We have $a^2 \equiv -b^2 \pmod p$. Since a, b are not divisible by p, we can use Legendre symbol:

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right).$$

By property 5, $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.