Solutions to Exam 1

Problem 1. a) State the Division Algorithm Theorem (3 points).

b) Using the Euclidean algorithm compute $\gcd(212, 148)$. Then find $x, y \in \mathbb{Z}$ such that $\gcd(212, 148) = x \cdot 212 + y \cdot 148$ (check your answer!). (4 points)

c) Let a be an integer. Prove that $\gcd(3a + 5, 7a + 12) = 1$. (4 ponts)

Solution: a)

b) Euclid's algorithm yields:

$$212 = 1 \cdot 148 + 64,$$

$$148 = 2 \cdot 64 + 20,$$

$$64 = 3 \cdot 20 + 4,$$

$$20 = 5 \cdot 4 + 0.$$

It follows that $\gcd(212, 148) = 4$. Working backwards,

$$4 = 64 - 3 \cdot 20 = 64 - 3 \cdot (148 - 2 \cdot 64) = 7 \cdot 64 - 3 \cdot 148 = 7 \cdot (212 - 1 \cdot 148) - 3 \cdot 148 = 7 \cdot 212 - 10 \cdot 148.$$

Thus $x = 7$, $y = -10$ work.

One can also use matrix computation to find x, y, see solution to problem 3 in homework 1.

c) 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 2. a) State the Chinese Remainder Theorem. (3 points)

b) Find all positive integers smaller than 300 which leave remainder $1, 3, 7$ upon division by $3, 5, 8$ respectively. Carefully explain all your work and reasoning. (4 points)

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 $0 < x < 300$ and

$$x \equiv 1 \pmod{3} \ , \ x \equiv 3 \pmod{5} \ , \ x \equiv 7 \pmod{8} \ .$$

In order to find a solution to these congruences, we follow the algorithm. We have $N = 3 \cdot 5 \cdot 8 = 120$, $N_1 = 40$, $N_2 = 24$, $N_3 = 15$.

We solve $N_1 x_1 \equiv 1 \pmod{3}$, i.e. $40x_1 \equiv 1 \pmod{3}$, which has a solution $x_1 = 1$.

Next we solve $N_2 x_2 \equiv 3 \pmod{5}$, i.e. $24x_2 \equiv 3 \pmod{5}$, which has a solution $x_2 = 2$.

Finally, we solve $N_3 x_3 \equiv 7 \pmod{8}$, i.e. $15x_3 \equiv 7 \pmod{8}$, which has a solution $x_3 = 1$.

A solution is given by $x = N_1x_1 + N_2x_2 + N_3x_3 = 40 + 48 + 15 = 103$. This is the smallest positive solution, since it is smaller than N. All solutions are given by the formula $x = 103 + 120m$, $m \in Z$. We get a positive solution smaller than 300 only for $m = 0, 1$. Thus 103 and 223 are the only solutions to our problem.

Problem 3. a) State Wilson's Theorem. (3 points)

b) Find the reminder upon division of 26! by 29. (4 points)

Solution. a) **Wilson's Theorem.** p is a prime number if and only if $(p-1)! \equiv -1 \pmod{p}$.

b) Since 29 is a prime number, we have $28! \equiv -1 \pmod{29}$ by Wilson's theorem. Let $x = 26!$ then $28! = x \cdot 27 \cdot 28$. Thus

$$-1 \equiv 28! = x \cdot 27 \cdot 28 \equiv x(-2)(-1) = 2x \pmod{29} .$$

Note that 15 is the inverse of 2 modulo 29 so

$$x \equiv 15(-1) = -15 \equiv 14 \pmod{29} .$$

Therefore the reminder upon division of 26! by 29 is equal to 14.

Problem 4. a) State Fermat's Little Theorem and Euler's Theorem. (4 points)

b) (4 points) Let p, q be distinct prime numbers. Prove that

$$p^q + q^p \equiv p + q \pmod{pq} .$$

c) Find the last 2 digits of 91^{2003}. (4 points)

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. Equivalently, $a^p \equiv a \pmod{p}$ for any integer a.

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. Here $\phi(n)$ is the number of positive integrs relatively prime to n and $\leq n$.

b) Since p and q are relatively prime, the congruence $p^q+q^p \equiv p+q \pmod{pq}$ is equivalent to the two congruences $p^q + q^p \equiv p + q \pmod{p}$ and $p^q + q^p \equiv p + q \pmod{q}$. The first of these congruences is equivalent to $q^p \equiv q \pmod{p}$, which is true by Fermat's Little Theorem. Similarly, the second of these congruences is equivalent to $p^q \equiv p \pmod{q}$, which again is true by Fermat's Little Theorem.

c) Finding the last two digits of a number n is the same as finding the reminder n leaves upond division by 100. Note that

$$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = 2 \cdot 20 = 40.$$

Since 91 is relatively prime to 100, we have $91^{40} \equiv 1 \pmod{100}$ by Euler's theorem. It follows that

$$91^{2003} = 91^{40\cdot 50+3} = (91^{40})^{50}\cdot 91^3 \equiv 1^{50}\cdot 91^3 \equiv (-9)^3 = (-9)\cdot 81 \equiv (-9)(-19) = 171 \equiv 71 \pmod{100}\ .$$

Thus the last 2 digits of 91^{2003} are 7 and 1.

Problem 5. a) Find the inverse of 7 modulo 26. (3 points)

b) (4 points) Find all incongruent modulo 28 solutions to the following congruence

$$18x \equiv 12 \pmod{28}\ .$$

c) Is the congruence $x^3 \equiv 6 \pmod{37}$ solvable? Explain your answer. (r points)

Solution. a) While it is not hard to find the inverse by hand, the proper algorithm is to perform Euclid's algorithm:

$$26 = 3\cdot 7 + 5,$$
$$7 = 1\cdot 5 + 2,$$
$$5 = 2\cdot 2 + 1,$$
$$2 = 2\cdot 1 + 0.$$

This tells us that 7 is relatively prime to 26 (hence the inverse modulo 26 exists) and working backwards, we get

$$1 = 5 - 2\cdot 2 = 5 - 2(7 - 1\cdot 5) = (-2)\cdot 7 + 3\cdot 5 = (-2)\cdot 7 + 3(26 - 3\cdot 7) = 3\cdot 26 - 11\cdot 7.$$

It follows that $-11 \equiv 15 \pmod{26}$ is the inverse of 7 modulo 26.

b) Using Euclid's algorithm we find that $\gcd(18, 28) = 2$. 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 $x \equiv 24 \pmod{28}$.

c) This problem asks whether 6 is a cubic residue modulo 37. Since 37 is a prime, a primitive root modulo 37 exists, and therefore 6 is a cubic residue modulo 37 if and only if

$$6^{\phi(37)/\gcd(3,\phi(37))} = 6^{12} \equiv 1 \pmod{37}$$

(we used here that $\phi(37) = 36$). Since $6^2 = 36 \equiv -1 \pmod{37}$, we have $6^{12} \equiv (-1)^6 = 1 \pmod{37}$. It follows that the congruence in question is solvable. In this particular case one can actually find a solution easily: since $6^2 \equiv -1 \pmod{37}$, multiplyting both sides by -6 yields $(-6)^3 \equiv 6 \pmod{37}$.

Problem 6. a) Define a primitive root modulo m. When does it exist? (4 points)

b) Find a primitive root modulo 18. Explain your answer. (3 points)

c) Show that if $\gcd(a, 600) = 1$ then 600 divides $a^{20} - 1$. (4 points)

d) (4 points) Suppose that $a^{20} - 1$ is divisible by m for every integer a relatively prime to m. Using the formula for the exponent of m prove that m is ot divisible by any prime larger than 11. **Extra credit.** Find the largest m with this property

Solution. A **primitive root modulo** m is any integer a such that $\gcd(a, m) = 1$ and $\text{ord}_m a = \phi(m)$. 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 $1 \leq k < \phi(m)$.

The **Primitive Root Theorem** says that a primitive root modulo m exists if and only if m is one of the numbers $2, 4, p^k, 2p^k$, where p is an odd prime and $k > 0$ an integer.

b) It is not hard to find a primitive root modulo 18 by hand, but we will follow the general startegy. Since $18 = 2 \cdot 3^2$, a primitive root modulo 18 exists. First we find a primitive root modulo 3. We see that 2 is a primitive root modulo 3. Since 9 does not divide $2^2 - 1$, 2 is a primitive root modulo any power of 3. In particular, 2 is a primitive root modulo 9. It is even though, so we need to add $3^2 = 9$ to get a primitive root modulo 18. Thus $11 = 2 + 9$ is a primitive root modulo 18.

c) Let a be any integer relatively prime to 600. Note that $600 = 2^3 \cdot 3 \cdot 5^2$. To show that 600 divides $a^{20} - 1$ it suffices to show that

$$a^{20} \equiv 1 \pmod{8}\ ,\ a^{20} \equiv 1 \pmod{3}\ ,\ a^{20} \equiv 1 \pmod{25}\ .$$

Since $\phi(8) = 4$, $\phi(3) = 2$, $\phi(25) = 20$ all divide 20, the three congruences follow immediately from Euler's theorem.

A different solution to the problem is to use the formula for exponenent of 600. We have

$$\text{exponent}(600) = \text{lcm}(\text{exponent}(8), \phi(3), \phi(25)) = \text{lcm}(2, 2, 20) = 20.$$

Thus $a^{20} \equiv 1 \pmod{600}$ for every integer a relatively prime to 600.

d) Suppose that $a^{20} - 1$ is divisible by m for every integer a relatively prime to m. This means that the exponenet of m divides 20. Write $m = 2^a p_1^{a_1} \dots p_s^{a_s}$, where $p_1 < p_2 < \dots < p_s$ are odd prime numbers. Then

$$\text{exponent}(m) = \text{lcm}(\text{exponent}(2^a), \phi(p_1^{a_1}), \dots, \phi(p_s^{a_s})).$$

If $a_i > 0$ then $\phi(p_i^{a_i})$ is divisible by $p_i - 1$. Thus $p_i - 1$ divides 20. We see that $p_i - 1$ can be $1, 2, 4, 5, 10, 20$, so the only possibilities for p_i are $2, 3, 5, 11$ (note that 21 is not a prime). This proves that no prime divisor of m can be larger than 11. To answer the extra credit question note that we have $m = 2^a 3^{a_1} 5^{a_2} 11^{a_3}$ and exponent of m divides 20 if and only if $\text{exponent}(2^a) | 20$, $\phi(3^{a_1}) = 2 \cdot 3^{a_1 - 1} | 20$, $\phi(5^{a_2}) = 4 \cdot 5^{a_2 - 1} | 20$, and $\phi(11^{a_3}) = 10 \cdot 11^{a_3 - 1} | 20$. This means that $a \leq 3$, $a_1 \leq 1$, $a_2 \leq 2$ and $a_3 \leq 1$. Thus the largest m is $2^3 \cdot 3 \cdot 5^2 \cdot 11 = 6600$.

Problem 7. Suppose that 10 is a primitive root modulo n. What can you say about the decimal expansion of $1/n$? (4 points)

Solution. If 10 is a primitive root modulo n then $\mathrm{ord}_n 10 = \phi(n)$ and $\gcd(n, 10) = 1$, so neither 2 nor 5 divide n. Thus the decimal expansion of $1/n$ is purely periodic with period of length $\phi(n)$.

Problem 8. Let p be an odd prime and $a > 1$ an integers such that p divides $a^8 + 1$.

a) What is the order of a modulo p? Explain your answer. (4 points)

b) Prove that $p \equiv 1 \pmod{16}$. (4 points)

Solution. a) We are given that $a^8 \equiv -1 \pmod{p}$. Thus $a^{16} \equiv 1 \pmod{p}$. This means that $\mathrm{ord}_p a | 16$. Note that $\mathrm{ord}_p a$ does not divide 8, since otherwise we would have $1 \equiv a^8 \equiv -1 \pmod{p}$, which is not possible. The only divisor of 16 which does not divide 8 is 16, so $\mathrm{ord}_p a = 16$.

b) Since we know from a) that $\mathrm{ord}_p a = 16$ and $a^{p-1} \equiv 1 \pmod{p}$ from Fermat's Little Theorem, we see that $\mathrm{ord}_p a = 16 | p - 1$. This means that $p \equiv 1 \pmod{16}$.

Problem 9. Is there a prime p such that each of the numbers $2, 3, 6$ is a primitive root modulo p? Justify your answer.

Solution: The answer is no. Indeed, recall that if g is a primitive root modulo p then $g^{(p-1)/2} \equiv -1 \pmod{p}$. Thus, if both 2 and 3 are primitive roots modulo p then $2^{(p-1)/2} \equiv -1 \pmod{p}$ and $3^{(p-1)/2} \equiv -1 \pmod{p}$. Multiplying these congruences, we get

$$6^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} 3^{\frac{p-1}{2}} \equiv (-1)(-1) = 1 \pmod{p} .$$

Thus 6 is not a primitive root modulo p.

Equivalently, note first that an even power of a primitive root cannot be a primitive root. But if both 2, 3 are congruent to odd powers of a chosen promitive root g then $6 = 2 \cdot 3$ would be congruent to an even power, hence would not be a primitive root modulo p.

Problem 10. Let p be a prime number such that $p+4$ and $p+8$ are also prime numbers. What is p? Justify your answer.

Solution: Note that one of the numbers p, $p + 4 = (p + 3) + 1$, $p + 8 = (p + 6) + 2$ must be divisible by 3. The only prime divisible by 3 is 3. So one of the numbers must be 3. This implies that $p = 3$, $p + 4 = 7$, $p + 8 = 11$.

Problem 11. Let $a > 1$ be an integer. Prove that if d divides both $a^n - 1$ and $a^m - 1$ then d divides $a^{\gcd(m,n)} - 1$. Conclude that

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1.$$

Hint: Consider the order of a modulo d.

Solution: Let $k = \mathrm{ord}_d a$. Since $a^n \equiv 1 \pmod{d}$ and $a^m \equiv 1 \pmod{d}$, we have $k | n$ and $k | m$. Thus $k | \gcd(n, m)$ and therefore $a^{\gcd(m,n)} \equiv 1 \pmod{d}$. This means that d divides $a^{\gcd(m,n)} - 1$. On the other hand, taking $d = a^{\gcd(m,n)} - 1$ we see that $a^{\gcd(m,n)} \equiv 1 \pmod{d}$. Thus $\mathrm{ord}_d a$ divides $\gcd(m, n)$, and therefore it divides both m and n. Thus $a^n \equiv 1 \pmod{d}$ and $a^m \equiv 1 \pmod{d}$. In other words, $a^{\gcd(m,n)} - 1$ divides both $a^n - 1$ and $a^m - 1$. We see that

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1.$$