Exam 1

Problem 1. a) Define $\gcd(a, b)$. Using Euclid's algorithm compute $\gcd(889, 168)$. Then 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 $\gcd(3a + 5, 7a + 12) = 1.$.

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 2. a) State the 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 $0 \le x < N$. 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) 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^{2018} 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. 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) 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 $\phi(36) = \phi(2^2)\phi(3^2) = 2 \cdot 2 \cdot 3 = 12$. Therefore $31^{12} \equiv 1 \pmod{36}$. Observe that $2018 = 12 \cdot 168 + 2$, so

$$31^{2018} = (31^{12})^{168} \cdot 31^2 \equiv 31^2 \pmod{36} .$$

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

Problem 4. Find all solutions to the following congruences

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

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 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 $1 \le k < \phi(m)$.

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:

$$2^2 = 4 \not\equiv 1 \pmod{25} ; \quad 2^4 = 16 \not\equiv 1 \pmod{25}$$

$$2^5 = 32 \equiv 7 \not\equiv 1 \pmod{25} ; \quad 2^{10} \equiv 7^2 \equiv -1 \not\equiv 1 \pmod{25} .$$

Thus the order of 2 modulo 25 is equal to 20 and therefore 2 is a primitive root modulo 25.

Second method: We proved in class the following result: if p is an odd prime and a is a primitive root modulo p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ then a is a primitive root modulo p^k for every positive integer k.

Taking $p = 5$, $a = 2$ we see that 2 is a primitive root modulo 5 and $2^4 \not\equiv 1 \pmod{25}$. Thus 2 is a primitive root modulo any power of 5.

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.

vspace3mm

Problem 6. Let $a > 1$, $n > 1$ be integers

a) What is the order of a modulo $a^n + 1$? Explain your answer.

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

Solution: a) Let t be the order of a modulo $a^n + 1$ (note that a and $a^n + 1$ are relatively prime). Clerly we have $a^n \equiv -1 \pmod{a^n + 1}$. Squaring we get $a^{2n} \equiv 1 \pmod{a^n + 1}$.

Thus $t|2n$. Any divisor of $2n$ less than $2n$ does not exceed n But if $t \leq n$ then $a^t - 1 \leq a^n - 1$, so $a^t - 1$ can not be divisible by $a^n + 1$. This means that $t = 2n$.

b) By Euler's Theorem, $a^{\phi(a^n+1)} \equiv 1 \pmod{a^n + 1}$. Thus $t|\phi(a^n + 1)$. Since $t = 2n$, the result follows.

Problem 7. Let p be a prime such that $p \equiv 2 \pmod 3$. Prove that the congruence $x^3 \equiv a \pmod p$ is solvable for every integer a. How many solutions modulo p does it have for a given a?

Solution: When $p|a$, then the congruence has a unique solution $a \equiv 0 \pmod p$.

Suppose that $p \nmid a$. We know that $x^3 \equiv a \pmod p$ is solvable if and only if $a^{(p-1)/\gcd(3,p-1)} \equiv 1 \pmod p$. Since $p \equiv 2 \pmod 3$, $p - 1$ is not divisible by 3, hence $\gcd(p - 1, 3) = 1$. Thus our condition is $a^{p-1} \equiv 1 \pmod p$, which is true by the Fermat Little Theorem.

What we proved so far is that the map $f(x) = x^3 \pmod p$ is a surjective map from $\{1, 2, \ldots, p - 1\}$ to itself. Thus, it has to be a bijection. In other words the congruence $x^3 \equiv a \pmod p$ gas unique solution for every a.

Second method: Let g be a primitive root modulo p, so $\mathrm{ord}_p(g) = p - 1$. Then $\mathrm{ord}_p(g^3) = (p - 1)/\gcd(3, p - 1) = p - 1$, so g^3 is also a primitive root modulo p. It follows that for every a relatively prime to p there is unique k such that $1 \leq k \leq p - 1$ and $a \equiv g^{3k} \pmod p$. In other words, there is unique $x = g^k$ solving $x^3 \equiv a \pmod p$.

Problem 8. 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:

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

We know that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.

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

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 divisor of $10^{10^n}+1$. Prove that 2^{n+1} divides $p-1$.

Solution: Note that $10^{10^n} = a^{2^n}$, where $a = 10^{5^n}$. We will show that if $a > 1$ and $p|a^{2^n}+1$ then 2^{n+1} divides $p-1$. Indeed, we have $a^{2^n} \equiv -1 \pmod{p}$, so $a^{2^{n+1}} \equiv 1 \pmod{p}$. Let t be the order of a modulo p. Thus t divides 2^{n+1}. We claim that $t = 2^{n+1}$. Otherwise, if $t < 2^{n+1}$ then t would divide 2^n and we would have $a^{2^n} \equiv 1 \pmod{p}$, which is false. Thus $t = 2^{n+1}$. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $t|p-1$. In other words, 2^{n+1} divides $p-1$.