MEETING 8 - REFLECTIONS ON CONGRUENCES AND PROOF IN NUMBER THEORY

In this meeting we will review and deepen earlier work: we will look at why The Euclidean Algorithm works, study various examples of proofs in numbers theory and especially prove something called Fermat's Little Theorem and Wilson's Theorem.

But first, some Peer Instruction!

Let us take another example of The Euclidean Algorithm in action: Find the multiplicative inverse of $\overline{11}$ in $\mathbb{Z}_{36}$ and then use that to find all integers such that $11x \equiv 7 \pmod{36}$.

Solution: We start by finding the greatest common divisor between 11 and 36, it is 1, but we search for s, t such that $s \cdot 11 + t \cdot 36 = 1$, then $\overline{s}$ will be the multiplicative inverse of $\overline{11}$ in $\mathbb{Z}_{36}$. The Euclidean Algorithm is carried out by repeated applications of the Division Algorithm:

$36 = 3 \cdot 11 + 3, \qquad 11 = 3 \cdot 3 + 2, \qquad 3 = 1 \cdot 2 + 1$, here we have reached the bottom (gcd=1) so we move up again:

$1 = 3 - 2 \cdot 1, \quad 1 = 3 - (11 - 3 \cdot 3) \cdot 1 \Leftrightarrow 1 = 4 \cdot 3 - 1 \cdot 11, \quad 1 = 4 \cdot (36 - 3 \cdot 11) - 1 \cdot 11, \quad 1 = 4 \cdot 36 - 13 \cdot 11.$

This means that $-13 \cdot 11 \equiv 1 \pmod{36}$, but what about if we want to have an s in the interval $0, 1, \ldots, 35$? Well, we can just use the rule that $x \cdot y \equiv 1 \pmod{n} \Leftrightarrow (x + k \cdot n) \cdot y \equiv 1 \pmod{n}$ so that we can write

$$-13 \cdot 11 \equiv 1 \pmod{36} \Leftrightarrow (36 - 13) \cdot 11 \equiv 1 \pmod{36} \Leftrightarrow 23 \cdot 11 \equiv 1 \pmod{36}$$

and from here we can say that $s = 23$ so that the multiplicative inverse of $\overline{11}$ in $\mathbb{Z}_{36}$ is $\overline{23}$.

Now we can solve the congruence equation $11x \equiv 7 \pmod{36}$. We begin by rewriting it in $\mathbb{Z}_{36}$. As $\overline{11}$ apparently has a multiplicative inverse in $\mathbb{Z}_{36}$ we can write the congruence as the equation

$$\overline{11} \cdot \overline{x} = \overline{7}$$

multiplying both sides with the multiplicative inverse of $\overline{11}$, which is $\overline{23}$ so that

$$\overline{11} \cdot \overline{x} = \overline{7} \Leftrightarrow \overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{23} \cdot \overline{7} \Leftrightarrow \overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{161} = \overline{17} \Leftrightarrow$$

$$\overline{23} \cdot \overline{11} \cdot \overline{x} = \overline{1} \cdot \overline{x} = \overline{x} = \overline{17}$$

So the result in $\mathbb{Z}_{36}$ is $\overline{17}$, so that the solutions to the original congruence is all the numbers on the form

$$17 + 36 \cdot k, \quad k = 0, \pm 1, \pm 2, \ldots.$$

Why does the Euclidean Algorithm work? Why do we always end up with the Greatest Common Divisor when we reduce two numbers by repeatedly using the Division Algorithm? It is due to this lemma:

Lemma: Let a, b be two positive integers with $b > a$. Then if the division algorithm is applied to yield

$$b = a \cdot q + r$$

where $0 \leq r < a$ and $q \geq 0$, then we have $\gcd(b, a) = \gcd(a, r)$.

By this lemma, we can start with any two positive numbers, b, a and reduce and eventually get down to the the greatest common divisor. This is what we have done so far. I now remains to prove this lemma.

Proof: Introduce two sets of positive integers:

$$A = \{d \in \mathbb{Z}^+; d|b \wedge d|a\} \quad \text{and} \quad B = \{d \in \mathbb{Z}^+; d|a \wedge d|r\}$$

that is all the positive common divisors to b, a and a, r respectively. These two sets are nonempty. (Why?) Then by definition $\gcd(b, a)$ is the largest element in A and $\gcd(a, r)$ is the largest element in B. But we shall prove that the two sets are in fact the same. Choose an element $d_1 \in A$. Then $d_1|b$ and $d_1|a$, so that we can write $b = k_1 \cdot d_1$ and $a = l_1 \cdot d_1$. We substitute this into the equation $b = a \cdot q + r$ yielding

$$k_1 \cdot d_1 = l_1 \cdot d_1 \cdot q + r \Leftrightarrow r = k_1 \cdot d_1 - l_1 \cdot d_1 \cdot q = d_1 \cdot (k_1 - l_1 \cdot q) \Rightarrow d_1|r$$

so that we have both $d_1|a$ and $d_1|r$, that is d_1 is a common divisor for a, r, that is we have $d_1 \in B$. Since this works for all common divisors in A we have $A \subseteq B$. But the exact same procedure can be done in reverse, by

choosing an element in B we can see that it is in A, that is, we can easily show that $B \subseteq A$. But then $A = B$ and the two largest elements, $\gcd(b, a)$ and $\gcd(a, r)$ must be the same.

We could of course also formulate a proof by not appealing to the notion of sets, but I think that it becomes a bit clear if we do use the notion of sets.

Let us look at two classic theorems:

Theorem: The smallest divisor greater than 1 (since 1 divides every number we do not really care about that) of any number greater than 1 must be a prime number.

Proof: Let $n > 1$ be any integer. We again introduce the set of all positive nontrivial divisors of n, this is the set

$$\{d > 1; d|n\}.$$

It is our task to show that the smallest element of this set is a prime number. If the number n itself is already a prime number then the set only has one element, namely n itself and since this is a prime number then smallest element (which is the only element) is a prime number. Assume that n is not a prime number, then we can write $n = a \cdot b$ for two integers $a > 1$ and $b > 1$ so we have show that the set is at least not empty. Since it has only positive numbers in it, it must have a smallest element. Call this element q. We want to show that q is a prime numeber. Assume that q is not a prime number, then there are, again, $a > 1, b > 1$ such that $q = a \cdot b$, but which a, b are possible? We know that $1 < a < q$ and $1 < b < q$, but since $a|q$ and $b|q$ and $q|n$, we must have both $a|n$ and $b|n$, but this means that we have found *smaller* divisors (two of the even! a, b are smaller divisors of n than q) that divides n. This contradicts our assumption that q was the smallest divisor greater than 1. This means that q must be a prime number which concludes the proof.

From this theorem follows an extremely important theorem:

Theorem: *Euclid* There are infinitely many prime numbers.

Proof: Assume that there is only a finite number of prime numbers, then we can put all of them in a list: $p_1, p_2, \ldots, p_n$ where n is some (possibly big) number. We know that $p_1 = 2$ and $p_2 = 3$ and that, according to the assumption, there are no prime numbers bigger than p_n. Then form the very big number

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Since this number is larger than p_n, which is the largest prime number, then N itself cannot be a prime number. Hence there must be a smallest number that divides this number and this must be a prime number according to the previous theorem, since we have a complete list of all the prime numbers we know that one of them must be this smallest prime that divides this n, that is we know that

$$p_1|N \quad \text{or} \quad p_2|N \quad \ldots \quad p_n|N.$$

But none of these divisions work, why? Well, N gives remainder 1 when divided by each of $p_1, p_2, \ldots, p_n$, that is the way we made N, so this is a contradiction, we have reached a contradiction and the impossible thing that led to this contradiction is the assumption that there is a finite number of prime numbers, which must be false. Hence there are infinitely many prime numbers which is what we wanted to prove.

This last theorem guarantees that we can form arbitrarily large keys in the RSA algorithm - which is good for our privacy and commerce.

We look at another important result:

Theorem: *(Fermat's Little Theorem)* If p is a prime number and $p \nmid c$, then

$$c^{p-1} \equiv 1 \pmod{p}.$$

Proof: By the previous proposition, no two integers $c, 2c, \ldots, (p-1)c$ are congruent modulo p. This means that in $\mathbb{Z}_p$ the elements $\overline{c}, \overline{2c}, \ldots, \overline{(p-1)c}$ are just the elements $\overline{1}, \overline{2}, \ldots, \overline{c}$ but possibly in another order. This means that

$$\overline{c} \cdot \overline{2c} \cdot \ldots \cdot \overline{(p-1)c} = \overline{c} \cdot \overline{2} \cdot \overline{c} \cdot \ldots \cdot \overline{(p-1)} \cdot \overline{c} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}$$

so that

$$c \cdot c \cdot \ldots \cdot c\overline{(p-1)!} = \overline{(p-1)!}$$

which gives (after "division" by $(p-1)!$) $c^{p-1} = \overline{1}$ which, written out as a congruence is $c^{p-1} \equiv 1 \pmod{p}$ which is what we wanted to prove.

During the last meeting we worked with pairing up the nonzero elements of $\mathbb{Z}_p$ where p is an odd prime i twos, the multiplicative inverse together. We will use this property now in the proof of another theorem:

Theorem: *(Wilson's Theorem)* For every prime number p we have

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof: In $\mathbb{Z}_p$, line up all nonzero elements and multiply them together: $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}$. What is this element? Well on one hand it is $\overline{(p-1)!}$, but we can also rearrange the product and pair up each element with its own multiplicative inverse. This is possible according to the above investigation, in $\mathbb{Z}_7$ it would look like this:

$$\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} = \overline{1} \cdot \overline{2} \cdot \overline{4} \cdot \overline{3} \cdot \overline{5} \cdot \overline{6} = \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{6} = \overline{6}$$

and in general it would look like this:

$$\overline{1} \cdot \ldots \cdot \overline{p-1} = \overline{1} \cdot \overline{1} \cdot \ldots \cdot \overline{1} \cdot \overline{p-1} = \overline{p-1}$$

so that

$$\overline{(p-1)!} = \overline{p-1}$$

but after rewriting this as a congruence it reads $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$ which is what we wanted to prove.