# Math 104a: Number theory – Problem set 5

François Thilmany

due Friday 3 August 2018

**Problem 1.** Complete the proof of the "if" direction of Wilson's theorem: $n \in \mathbb{N} - \{0,1\}$ is prime if (and only if)

$$(n-1)! \equiv -1 \mod n.$$

Hint: Suppose that $n$ is composite. Prove that if $n$ can be factored $n = ab$ with $a, b \in \mathbb{N}$ and $a \neq b$, then $(n-1)! \equiv 0 \mod n$ (this had been done in class, briefly reproduce the argument). If $n$ cannot be factored as above, show that $n$ must be the square of a prime number $p > 0$. If $p = 2$, then of course $(n-1)! = 2 \mod n$. If $p > 2$, show that $(n-1)! = 0 \mod n$.

**Problem 2.** Let $p > 0$ be a prime number and let $y \in \mathbb{Z}_p^\times$ have (multiplicative) order $m$. If $m$ is even, show that $y^{m/2} = -1$. Does this still hold without the assumption that $p$ is prime?

Hint: Show that $y^{m/2}$ is a root of the polynomial $X^2 - 1$.

**Problem 3.** Let $p > 0$ be an odd prime. Prove that $-1$ is a square in $\mathbb{Z}_p$ if and only if $p \equiv 1 \mod 4$.

Hint: if $-1$ is a square in $\mathbb{Z}_p$, show that $\mathbb{Z}_p^\times$ has an element of order 4.

**Problem 4.** Let $p > 0$ be an odd prime and pick a generator $x$ of the cyclic group $\mathbb{Z}_p^\times$. Prove that $-x$ is a generator of $\mathbb{Z}_p^\times$ if and only if $p \equiv 1 \mod 4$.

**Problem 5.** Suppose that $m \in \mathbb{N} - \{0,1\}$ is such that $\mathbb{Z}_m^\times$ is cyclic. Determine the number of different generators of $\mathbb{Z}_m^\times$.

**Problem 6.** Let $m, n > 1$ be integers such that $n \mid m$.

(a) Show that

$$\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x + m\mathbb{Z} \mapsto x + n\mathbb{Z}$$

is a well-defined, surjective ring homomorphism.

(b) Compute the kernel of $\phi$.

**Problem 7.** (a) If $\psi : R \to S$ is any homomorphism of rings, show that $\psi$ restricts to a homomorphism of groups $\psi^\times : R^\times \to S^\times$.

(b) If $\psi : R \to S$ is surjective, is $\psi^\times : R^\times \to S^\times$ necessarily surjective? Prove this or provide a counterexample.

(c) Let $m \geq n > 0$ be integers. Prove that the canonical map (from problem 6)

$$\phi : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} : x + p^m\mathbb{Z} \mapsto x + p^n\mathbb{Z}$$

does restrict to a surjective homomorphism of groups $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.

**Problem 8.** Let $G$ be a commutative group and $a, b \in G$ elements of orders $m$ and $n$ respectively.

(a) Show that the order of $ab$ divides $\text{lcm}(m, n)$.

(b) Prove that if $\gcd(m, n) = 1$, then the order of $ab$ is $mn$ $(= \text{lcm}(m, n))$.

(c) Give an example for which the order of $ab$ is not equal to $\text{lcm}(m, n)$.

**Problem 9.** (a) Compute the orders of 2 and 7 in $\mathbb{Z}_{73}^\times$.

(b) Find a generator of the cyclic group $\mathbb{Z}_{73}^\times$.

(c) Find a generator of the cyclic group $\mathbb{Z}_{146}^\times$.

**Problem 10.** Prove that 2 is a generator of $\mathbb{Z}_{3^n}^\times$ for any $n \in \mathbb{N} - \{0\}$.

Hint: Compute the order of 2 in $\mathbb{Z}_{3^n}^\times$.

**Problem 11.** Find all generators of $\mathbb{Z}_{25}^\times$.

Hint: Lift the generators of $\mathbb{Z}_5^\times$ to elements in $\mathbb{Z}_{25}^\times$, then compute their (multiplicative) orders. If one of the lifts, say $a \in \mathbb{Z}_{25}^\times$, is not a generator, use an argument from class to show that $a + k5$ is a generator for $k \in \{1, 2, 3, 4\}$. If needed, verify that you have the right number of generators using problem 5.

**Problem 12.** Let $p > 0$ be an odd prime. Show that exactly $\frac{p-1}{2} + 1$ elements of $\mathbb{Z}_p$ are squares.

Hint: Of course, 0 is a square. Show that the 'square' map $s : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times : x \mapsto x^2$ is two-to-one, that is, the preimage $s^{-1}(y)$ of any element $y$ in $\mathbb{Z}_p^\times$ consists of exactly two (distinct) elements. Use this to count the size of the image of $s$.

Here is another way: after identifying the (cyclic) multiplicative group $\mathbb{Z}_p^\times$ with the additive group $\mathbb{Z}_{p-1}$, show that the squares correspond to even residues.

**Problem 13.** Let $p > 0$ be an odd prime and pick $a, b, c \in \mathbb{Z}_p$ with $a \neq 0$. Prove that the polynomial $ax^2 + bx + c$ has a root in $\mathbb{Z}_p$ if and only if $b^2 - 4ac$ is a square in $\mathbb{Z}_p$. If $\delta \in \mathbb{Z}_p$ is such that $\delta^2 = b^2 - 4ac$, prove that the usual formula $\frac{-b \pm \delta}{2a}$ yields the two roots of $ax^2 + bx + c$.

Hint: Complete the square. Because $p$ is an odd prime, 2 and $a$ are invertible in $\mathbb{Z}_p$. You do not need to actually compute the inverse of 2 (nor of $a$) to complete the square.

For the two last problems, you might need the law of quadratic reciprocity. We will state it on Wednesday.

**Problem 14.** Determine whether:
(a) 8 is a square in $\mathbb{Z}_{97}$
(b) 5 is a square in $\mathbb{Z}_{97}$
(c) 30 is a square in $\mathbb{Z}_{97}$
(d) 501 is a square in $\mathbb{Z}_{773}$.
(e) 503 is a square in $\mathbb{Z}_{773}$.

**Problem 15.** Use problem 13 to quickly determine if the polynomial $x^2 + 5x + 3$ has a root
(a) in $\mathbb{Z}_{11}$
(b) in $\mathbb{Z}_{13}$
(c) in $\mathbb{Z}_{97}$.