Wilson’s theorem

**Theorem 1.** Let $p$ be prime. Then $(p - 1)! \equiv -1 \pmod{p}$.

**Remark.** John Wilson found the theorem without proof. Lagrange proved it in 1771 (together with the trivial converse: if $n$ divides $(n - 1)! + 1$ then $n$ is prime).

**Proof.** The product of all elements in a finite Abelian group equals the product of all elements of order 2. (Why?) Now in $\mathbb{Z}_p$ ($p$ prime), the only element of order 2 is -1, that is, the only solutions to $x^2 - 1 = 0$ are 1 and -1. $\square$

The last sentence in the proof was easy to see, since $x^2 - 1 = 0$ in $\mathbb{Z}_p$ means that $p$ divides $x^2 - 1 = (x - 1)(x + 1)$, hence $p$ must divide either $(x - 1)$ or $(x + 1)$. Alternatively, we could argue that 1 and -1 are obviously solutions to $x^2 - 1 = 0$, and a quadratic equation cannot have more than two solutions. Is this a valid argument in $\mathbb{Z}_p$? Would it be valid in $\mathbb{Z}_m$? The following theorem is from the handout *polynomials and field extensions*.

**Theorem 2.** In a field, an algebraic equation of degree $n \geq 1$ can have at most $n$ solutions (a polynomial of degree $n$ can have at most $n$ roots even with multiplicity).

How about roots of polynomials in $\mathbb{Z}_m$ for a composite $m$? (Note: $\mathbb{Z}_m$ is *not* a field.)

Example: Let $a, b > 1$, and let $m = ab > 4$. Then the quadratic equation $x(x - a - b) = 0$ has at least three solutions in $\mathbb{Z}_m$: $x = 0, a + b, a, b$. (Why three? Isn’t this four?)

HW: Prove that in an Abelian group, the set of all elements of order $\leq 2$ form a subgroup. (Can you generalize it?) [Hint: Use the standard (multiplicative) subgroup tests: 1. the set is closed under multiplication; 2. the set is closed under inverse.]

HW: In a **finite** group, the first subgroup test alone is enough, that is: If $(G, \cdot)$ is a finite group and $H$ is a non-empty subset of $G$ closed under multiplication, then $H$ is a subgroup.
Fermat’s “little theorem”

Theorem 3. Let $p$ be prime and $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

In general, let $m > 1$ and let $\varphi(m)$ denote the number of positive integers less than $m$ which are coprime to $m$ (Euler function). If $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Remark. The first statement (for prime $p$) was found by Fermat but proved by Euler, who generalized it to arbitrary moduli $m$.

Proof. The theorem is a simple consequence of the following lemma, and the fact that $\mathbb{Z}^*_m$ is an Abelian group, where $\mathbb{Z}^*_m$ is $\mathbb{Z}_m$ restricted to all its invertible elements.

Lemma 4. If $G$ is an Abelian group of order $n$ and identity $e$, then $a^n = e$ for all $a \in G$.

Proof. Let $a \in G$ be arbitrary. The map $f : G \to G : g \to ag$ is clearly a bijection, and hence,

$$ \prod_{g \in G} g = \prod_{g \in G} (ag) = a^{|G|} \prod_{g \in G} g $$

Remark. The conclusion of the Lemma is true for finite non-Abelian groups also (this is Lagrange’s theorem), as stated in the handout groups and fields, but for the proof of this general theorem one needs the notion of cosets.