Wilson's theorem, Fermat's little theorem and the Chinese remainder theorem

Sebastian Björkqvist

November 28, 2013

Abstract

This text presents and proves Wilson's theorem, Fermat's little theorem, and the Chinese remainder theorem.

Remark. In this text we notate elements in the quotient ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ by $\overline{x}$, i.e. by overlining them.

We begin by proving a lemma which will come in handy when we're proving Wilson's theorem. The lemma says that every integer that is not divisible by a prime number p has a multiplicative inverse modulo p.

Lemma 1. *Let p be a prime number and n be an integer. If $p \nmid n$, i.e. p does not divide n, then there exists an integer m such that*

$$nm \equiv 1 \pmod{p}.$$

The number m is also unique modulo p.

Proof. Existence: We notice that the statement $nm \equiv 1 \pmod{p}$ is true if and only if there exists an integer $k \in \mathbb{Z}$ for which it holds that $nm = 1 - kp$. Thus, if we wish to find a multiplicative inverse m for the integer n, we only need to solve the linear Diophantine equation

$$nm + kp = 1.$$

Since p is prime and $p \nmid n$, we know that $\gcd(p, n) = 1$. Thus, because $\gcd(p, n) \mid 1$, a solution (m, k) to the equation may be found using Euclid's algorithm, and it follows that $nm = 1 - kp \equiv 1 \pmod{p}$.

Uniqueness: Assume that we have another number m' for which it holds that $nm' \equiv 1 \pmod{p}$. It follows that $nm \equiv nm' \pmod{p}$, and thus $nm = nm' + kp$ for some integer k. Now $nm - nm' = kp$, and because n divides the left side of the equation, it must also divide the right side. Since p is a prime and $n \neq p$, n must divide k. The equation now takes the form

$$nm - nm' = nk'p,$$

where $k' = \frac{k}{n}$. Dividing by n gives us $m - m' = k'p$, which proves the claim.

□

Using the lemma above we may easily prove the following theorem about the quotient rings $\mathbb{Z}/n\mathbb{Z}$:

Theorem 2. *The ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Proof. "$\Leftarrow$" Assume that n is a prime number. Given any number $0 \neq \overline{m} \in \mathbb{Z}_n$, we use Lemma 1 and find a number $k \in \mathbb{Z}$ for which $mk \equiv 1 \pmod{p}$, and thus $\overline{m}\overline{k} = \overline{mk} = \overline{1}$.

"$\Rightarrow$" Assume that n is a composite number. Then we may find numbers a and b such that $a, b > 1$ and $n = ab$. It follows that $\overline{a}\overline{b} = \overline{ab} = \overline{n} = \overline{0}$, and thus we've found zero divisors in $\mathbb{Z}_n$. Thus $\mathbb{Z}_n$ is not an integral domain, and therefore it is not a field. □

Theorem 3. *(Wilson's theorem)*

$$(n-1)! \equiv -1 \pmod{n} \text{ if and only if } n \text{ is prime.}$$

Proof. "$\Leftarrow$" Let n be prime. Lemma 1 says that every number m for which it holds that $n \nmid m$ has a unique multiplicative inverse modulo n. Obviously $1 \cdot 1 \equiv 1 \pmod{n}$ and $(n-1)(n-1) \equiv -1 \cdot (-1) \equiv 1 \pmod{n}$, so the numbers 1 and $n-1$ are their own multiplicative inverses.

The numbers $2, 3, \ldots, n-2$ also have unique multiplicative inverses modulo n, and none of them can be their own inverse, since the equation $x^2 - 1 = 0$ is equivalent to the equation $(x-1)(x+1) = 0$, and for this equation to hold, either $x-1$ or $x+1$ must be zero, since Theorem 2 states that $\mathbb{Z}_n$ is a field and thus an integral domain.

This means we can pair every number $2, 3, \ldots, n-2$ with its inverse which isn't the number itself, but must lie in the same range. Since there is an even number of these numbers, it holds that $2 \cdot 3 \cdot \cdots \cdot (n-1) \equiv -1 \pmod{n}$, and thus $(n-1)! \equiv n-1 \equiv -1 \pmod{n}$.

"$\Rightarrow$" Assume that n is a composite number. We may now find numbers a and b such that $a, b > 1$ and $n = ab$. Obviously it also holds that $a, b < n$, so the product $(n-1)!$ contains both a and b. Since $ab \equiv 0 \pmod{n}$, it follows that $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$. □

Lemma 4. *Let p be a prime number, and let a be an integer for which it holds that $p \nmid a$, i.e. $\overline{0} \neq \overline{a} \in \mathbb{Z}_p$. Then*

$$\left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\} = \left\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\right\}.$$

In other words, multiplying all elements except $\overline{0}$ in the field $\mathbb{Z}_p$ with a non-zero element $a \in \mathbb{Z}_p$ creates an permutation of the elements, but the set doesn't change.

Proof. Since p is a prime, $\overline{a}$ has an unique multiplicative inverse $\overline{a^{-1}}$ by Lemma 1. Thus, if $\overline{ma} = \overline{na}$, it follows that $\overline{maa^{-1}} = \overline{naa^{-1}}$, which implies that $\overline{m} = \overline{n}$. Thus $\overline{ma} \neq \overline{na}$ if $\overline{m} \neq \overline{n}$, which means that the latter set has the same number of elements as the former, and every element in the latter set is distinct. Since $\overline{a} \neq \overline{0}$, none of the elements in the latter set is $\overline{0}$, and thus the sets must be equal. □

We may now prove easily Fermat's little theorem by using the results above:

Theorem 5. *(Fermat's little theorem)*

$$\textit{If } p \textit{ is prime and } p \nmid a, \textit{ then } a^{p-1} \equiv 1 \pmod{p}.$$

Proof. We see that

$$-1 \overset{Wilson}{\equiv} (p-1)! \overset{L.4}{\equiv} a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv a^{p-1}(p-1)! \overset{Wilson}{\equiv} -a^{p-1} \pmod{p},$$

and thus $a^{p-1} \equiv 1 \pmod{p}$. □

Remark. We notice that both Wilson's and Fermat's theorem gives us a way to find out if a number is prime without looking at its factorization. This proves to be useful when designing algorithms that determine if a number is prime or not.

Finally, we prove the Chinese remainder theorem.

Theorem 6. *(Chinese remainder theorem) Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, and assume that $\gcd(n_i, n_j) = 1$ for every $i, j \in 1, \ldots, k, i \neq j$. Then, for any given sequence $a_1, a_2, \ldots, a_k$ of integers there exists an integer b for which it holds that*

$$\begin{aligned} b &\equiv a_1 \pmod{n_1}, \\ b &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ b &\equiv a_k \pmod{n_k}. \end{aligned}$$

Also, all solutions of this system are congruent modulo $n_1 n_2 \cdots n_k$.

Proof. First, let us assume that we only have two integers n_1 and n_2, and let a_1 and a_2 be arbitrary integers. Assume that there are integers k and k' for which it holds that $a_1 + kn_1 \equiv a_1 + k'n_1 \pmod{n_2}$. It follows that $kn_1 \equiv k'n_1 \pmod{n_2}$, and thus it holds that $(k - k')n_1 \equiv 0 \pmod{n_2}$. This means that $(k - k')n_1 = ln_2$ for some $l \in \mathbb{Z}$, and because $\gcd(n_1, n_2) = 1$, we know that n_2 must divide $k - k'$. Thus, no number in the set

$$\{a_1 + kn_1 \mid k \in 0, 1, \ldots, n_2 - 1\}$$

is congruent to any other number in the set modulo n_2. Since the set has exactly n_2 elements, there must exist a k for which it holds that $a_1 + kn_1 \equiv a_2 \pmod{n_2}$. Obviously $a_1 + kn_1 \equiv a_1 \pmod{n_1}$, so we've found the desired number. If there exists two integers b and b' that satisfy the system, we know that $b \equiv b' \pmod{n_1}$ and $b \equiv b' \pmod{n_2}$. Thus we know that $n_1 | (b - b')$, and that $n_2 | (b - b')$. Because $\gcd(n_1, n_2) = 1$, it follows that $n_1 n_2 | (b - b')$, and thus $b \equiv b' \pmod{n_1 n_2}$.

Now that we've proven that the Chinese remainder theorem holds for two coprime integers, we notice that the proof for an arbitrary number of integers follows, because we may first find a solution b_{12} for which it holds that $b_{12} \equiv a_1 \pmod{n_1}$ and $b_{12} \equiv a_2 \pmod{n_2}$. After that we may replace the first two equations in the system by the equation $b \equiv b_{12} \pmod{n_1 n_2}$, and repeat the previous step, since $\gcd(n_1 n_2, n_1) = 1$ for every $i \in 3, \ldots, k$. After $k - 1$ steps we obtain a number b_{1k} that satisfies the system. □