Residue Classes with Order 1 or 2 and a Generalisation of Wilson's Theorem

Yimin Ge

Vienna, Austria

1 Introduction

We start off with a very famous theorem and the usual proof of it:

Theorem 1 (Wilson's Theorem)**.** *Let m be a positive integer. Then*

$$(m-1)! \equiv -1 \pmod{m}$$

if and only if m is a prime number.

Proof. Suppose first that $(m-1)! \equiv -1 \pmod{m}$ for some positive integer m. If m is not prime then there exists a divisor d of m with $1 < d < m$, so $d|(m-1)!$. But $d|m$, so $d|-1$, a contradiction. Thus, m must be prime.
Suppose now that m is prime. If some residue class x modulo m has got a multiplicative inverse[1] x^{-1} with $x \not\equiv x^{-1} \pmod{m}$ then they both drop out of $(m-1)!$. Hence, $(m-1)!$ is congruent to the product of all integers x with $1 \leq x \leq m-1$ and $x^2 \equiv 1 \pmod{m}$. However, since m is prime,

$$\begin{aligned} x^2 &\equiv 1 \pmod{m} \\ \Leftrightarrow (x-1)(x+1) &\equiv 0 \pmod{m} \\ \Leftrightarrow x \equiv 1 \pmod{m} \quad &\text{or} \quad x \equiv m-1 \pmod{m}. \end{aligned}$$

Hence,

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

□

[1] The *multiplicative inverse* of an integer x modulo a positive integer m is an integer x^{-1} modulo m which satisfies $xx^{-1} \equiv 1 \pmod{m}$. It is well known that x^{-1} exists if and only if $\gcd(x, m) = 1$ and furthermore if x^{-1} exists then it is unique modulo m.

2 A Generalisation of Wilson's Theorem

While the *only if*-part is trivial, the proof of the *if*-part of Wilsons's Theorem contains certain thoughts which can be adapted for one of the many generalisations of Wilson's Theorem, which is usually credited with Euler.

Proposition 1. *Let $m \geq 2$ be a positive integer and let $T(m)$ be the product of all integers x with $1 \leq x \leq m$ and $\gcd(x, m) = 1$, that is,*

$$T(m) := \prod_{\substack{1 \leq x \leq m \\ \gcd(x,m)=1}} x.$$

Then

$$T(m) \equiv \begin{cases} -1 & \text{if } m = 2, 4, p^k, 2p^k \\ 1 & \text{else} \end{cases} \pmod{m},$$

where p is an odd prime number and k a positive integer.

The trained eye will recognize the numbers m for which $T(m) \equiv -1 \pmod{m}$ as exactly the numbers modulo which primitive roots exist. A more detailled relation between these results requires deeper knowledge of algebra (in particular group theory) and is rudimentarily discussed in Section 3.
The main idea of the proof of Proposition 1 is very similar to the proof of the *if*-part of Wilson's Theorem, for the concrete implementation, we however shall require some more theory.

Defninition 1. Let $m \geq 2$ be a positive integer. Then $A(m)$ denotes the set of all integers x coprime to m with $1 \leq x \leq m$ having order[2] 1 or 2, that is

$$A(m) := \{x \in \mathbb{Z} \mid 1 \leq x \leq m, x^2 \equiv 1 \pmod{m}\}.$$

Let furthermore $\alpha(m) := |A(m)|$ and let $P(m)$ be the product of all elements in $A(m)$, that is,

$$P(m) := \prod_{x \in A(m)} x.$$

The first step in proving Proposition 1 is reducing $T(m)$ to $P(m)$, as we have done it in the proof of Theorem 1.

[2]The *order* of an integer x modulo m is the least positive integer t so that $x^t \equiv 1 \pmod{m}$. It exists if and only if $\gcd(x, m) = 1$ and is denoted by $\mathrm{ord}_m(x)$.

Lemma 1. *Let $m \geq 2$ be an integer. Then*

$$T(m) \equiv P(m) \pmod{m}.$$

Proof. Suppose that $x \in \{1, \ldots, m\}$ is an integer coprime to m. If the multiplicative inversive x^{-1} of x satisfies $x \not\equiv x^{-1} \pmod{m}$, then both x and x^{-1} drop out of $T(m)$. Thus, the only numbers left in $T(m)$ are those residue classes modulo m which are their own multiplicative inversives respectively and the set of those residue classes is defined as $A(m)$. $\square$

Notice that if $m \geq 3$ is an integer, then $\alpha(m)$ is even since if $x^2 \equiv 1 \pmod{m}$, then we also have $(-x)^2 \equiv 1 \pmod{m}$. It is also easy to see that

Lemma 2. *Let $m \geq 3$ be a positive integer. Then*

$$P(m) \equiv (-1)^{\alpha(m)/2}.$$

Proof. We have

$$\begin{aligned} P(m) &= \prod_{x \in A(m)} x = \prod_{\substack{1 \leq x \leq m \\ m|(x^2-1)}} x \equiv \prod_{\substack{1 \leq x \leq \lfloor \frac{m}{2} \rfloor \\ m|(x^2-1)}} x(-x) \\ &= \prod_{\substack{1 \leq x \leq \lfloor \frac{m}{2} \rfloor \\ m|(x^2-1)}} -x^2 \equiv \prod_{\substack{1 \leq x \leq \lfloor \frac{m}{2} \rfloor \\ m|(x^2-1)}} -1 = (-1)^{\alpha(m)/2} \pmod{m}. \end{aligned}$$ $\square$

We thus see that when analyzing $P(m)$, it is not necessary to know the exact residue classes in $A(m)$ but sufficient to know only the number of them. In the following, we will find a general formula for $\alpha(m)$.

Lemma 3. *We have $\alpha(1) = 1, \alpha(2) = 1, \alpha(4) = 2$.*

Proof. This directly follows from a trivial inspection: we have $A(1) = \{1\}$, $A(2) = \{1\}$ and $A(4) = \{1, 3\}$. $\square$

Lemma 4. *Let $k \geq 3$ be an integer. Then $\alpha(2^k) = 4$.*

Proof. Notice that x must be odd in order to be in $A(2^k)$. We have

$$\begin{aligned} & x^2 \equiv 1 \pmod{2^k} \\ \Leftrightarrow\ & (x-1)(x+1) \equiv 0 \pmod{2^k}. \end{aligned} \tag{1}$$

Since $x-1$ and $x+1$ are two consecutive even integers, (1) is equivalent to

$$x \equiv 1 \pmod{2^{k-1}} \quad \text{or} \quad x \equiv -1 \pmod{2^{k-1}}$$

and working modulo 2^k, this is equivalent to

$$x \equiv 1, 2^{k-1}-1, 2^{k-1}+1, 2^k-1 \pmod{2^k}.$$

Since $k \geq 3$, these four numbers are incongruent, so it follows that

$$A(2^k) = \{1, 2^{k-1}-1, 2^{k-1}+1, 2^k-1\}$$

and hence, $\alpha(2^k) = 4$. □

Lemma 5. *Let p be an odd prime number and let k be a positive integer. Then $\alpha(p^k) = 2$.*

Proof. We have

$$\begin{aligned} x^2 &\equiv 1 \pmod{p^k} \\ \Leftrightarrow (x-1)(x+1) &\equiv 0 \pmod{p^k}. \end{aligned} \tag{2}$$

Since p is an odd prime number, $x-1$ and $x+1$ cannot be both divisible by p. Thus, (2) is equivalent to

$$x \equiv 1, -1 \pmod{p^k},$$

so

$$A(p^k) = \{1, p^k - 1\}$$

and hence, $\alpha(p^k) = 2$. □

It thus remains to find $\alpha(m)$ for composite numbers m.

Lemma 6. *The function α is multiplicative, that is, for all positive integers m, n with $\gcd(m,n) = 1$ we have*

$$\alpha(mn) = \alpha(m)\alpha(n).$$

Proof. Suppose that $y_1, \dots, y_{\alpha(m)} \in A(m)$ and $z_1, \dots, z_{\alpha(n)} \in A(n)$ are the residues modulo m and n with order 1 or 2 respectively. Then $x^2 \equiv 1 \pmod{mn}$ holds if and only if

$$x \equiv y_i \pmod{m} \quad \text{and} \quad x \equiv z_j \pmod{n}$$

for some integer i with $1 \leq i \leq \alpha(m)$ and some integer j with $1 \leq j \leq \alpha(n)$. Obviously there are $\alpha(m)\alpha(n)$ ways to choose such a pair (i, j) and since we get a different residue modulo mn in $A(mn)$ for different pairs (i, j) by the chinese remainder theorem[3], we obtain $\alpha(mn) = \alpha(m)\alpha(n)$. $\square$

From Lemma 3 to 6, we obtain the following formula for $\alpha(m)$:

Theorem 2. *Let $m = 2^k p_1^{k_1} \dots p_r^{k_r}$ be the prime factorization of a positive integer m ($r \geq 0, k \geq 0, k_i \geq 1$). Then*

$$\alpha(m) = \begin{cases} 2^r & \text{if } k \leq 1 \\ 2^{r+1} & \text{if } k = 2 \\ 2^{r+2} & \text{if } k \geq 3. \end{cases}$$

From this formula, we immediately infer

Corollary 1. *Let $m \geq 2$ be an integer. Then $\alpha(m)$ is not divisible by 4 if and only if $m = 2, 4, p^k, 2p^k$, where p is an odd prime number and k is a positive integer.*

It follows now from Corollary 1, Lemma 1 and Lemma 2 that

$$T(m) \equiv P(m) \equiv \begin{cases} -1 & \text{if } m = 2, 4, p^k, 2p^k \\ 1 & \text{else} \end{cases} \pmod{m},$$

which proves Proposition 1. $\square$

[3]The *Chinese Remainder Theorem* states that if $m_1, \dots, m_r$ are pairwise coprime positive integers and $x_1, \dots, x_r$ are arbitrary integers, then the system of congruences

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ &\vdots \\ x &\equiv x_r \pmod{m_r} \end{aligned}$$

has an integer solution in x. Furthermore, this solution is unique modulo $m_1 \dots m_r$.

3 Prospects

From a much more advanced point of view, we know from the Chinese Remainder Theorem that

$$(\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^*$$

holds for any positive integer $m \geq 2$ having the canonical prime factorization $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$.
Furthermore,

$$(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^* \simeq \begin{cases} \mathcal{C}_{\varphi(p_i^{\alpha_i})} & \text{if primitive roots modulo } p_i^{\alpha_i} \text{ exist} \\ \mathcal{C}_{2^{\alpha_i-2}} \times \mathcal{C}_2 & \text{if } p_i = 2 \text{ and } \alpha_i \geq 3, \end{cases}$$

where $(\mathcal{C}_a, \cdot) \simeq (\mathbb{Z}/a\mathbb{Z}, +)$ is a cyclic group of order a in multiplicative notation.
However, $\varphi(p_i^{\alpha_i})$ is either 1 or even, so if we assume that $m > 2$ (which means $(\mathbb{Z}/m\mathbb{Z})^*$ is nontrivial), then we have found a decomposition of $(\mathbb{Z}/m\mathbb{Z})^*$ into cyclic groups of even order, that is,

$$(\mathbb{Z}/m\mathbb{Z})^* \simeq \mathcal{C}_{m_1} \times \ldots \times \mathcal{C}_{m_k},$$

where $m_1, \ldots, m_k$ are even positive integers. Indeed, we can assume that $m_1, \ldots, m_k$ are even positive integers since the trivial group $\mathcal{C}_1 \simeq (\mathbb{Z}/2\mathbb{Z})^*$ drops out of this decomposition if it exists.
In this configuration, $(\mathbb{Z}/m\mathbb{Z})^*$ is obviously cyclic if and only if $k = 1$ since $\mathcal{C}_{ab} \simeq \mathcal{C}_a \times \mathcal{C}_b$ holds if and only if $\gcd(a, b) = 1$.
Suppose now that $g_1, \ldots, g_k$ are generators of $\mathcal{C}_{m_1}, \ldots, \mathcal{C}_{m_k}$ respectively. As usual, we identify g_i as the tupel $(\underbrace{1, \ldots, 1}_{i-1}, g_i, \underbrace{1, \ldots, 1}_{k-i})$. Then

$$\prod_{x \in (\mathcal{C}_{m_1} \times \ldots \times \mathcal{C}_{m_k})} x = \prod_{\substack{0 \leq i \leq k \\ 0 \leq a_i < m_i}} g_1^{a_1} \ldots g_k^{a_k}.$$

For every integer a_i with $0 \leq a_i \leq m_i$, $g_i^{a_i}$ appears exactly $m_1 \ldots m_k / m_i$

times in this product. Hence,

$$\prod_{\substack{i=1,\ldots,k\\ 0\le a_i<m_i}} g_1^{a_1}\ldots g_k^{a_k} = g_1^{\frac{m_1\ldots m_k}{m_1}\sum_{a_1=0}^{m_1} a_1}\ldots g_k^{\frac{m_1\ldots m_k}{m_k}\sum_{a_k=0}^{m_k} a_k}$$
$$= g_1^{\frac{m_1\ldots m_k}{m_1}\frac{m_1(m_1-1)}{2}}\ldots g_k^{\frac{m_1\ldots m_k}{m_k}\frac{m_k(m_k-1)}{2}}$$
$$= g_1^{\frac{m_1\ldots m_k(m_1-1)}{2}}\ldots g_k^{\frac{m_1\ldots m_k(m_k-1)}{2}}.$$

But $g_1^{l_1}\ldots g_k^{l_k}=1$ holds if and only if $m_i|l_i$ for all $i=1,\ldots,k$ since we are working with a direct product. Thus,

$$g_1^{\frac{m_1\ldots m_k(m_1-1)}{2}}\ldots g_k^{\frac{m_1\ldots m_k(m_k-1)}{2}}=1$$

holds if and only if we have

$$m_i|\frac{m_1\ldots m_k}{2}(m_i-1) \tag{3}$$

for all $i=1,\ldots,k$. But we know that $m_1,\ldots,m_k$ are even, so (3) holds if and only if $k>1$ which in other words means that $(\mathbb{Z}/m\mathbb{Z})^*$ is not cyclic. If $k=1$ then

$$m_1\nmid\frac{m_1(m_1-1)}{2}\quad\text{but}\quad\frac{m_1}{2}|\frac{m_1(m_1-1)}{2},$$

so

$$\frac{m_1(m_1-1)}{2}\equiv\frac{m_1}{2}\pmod{m_1}.$$

Thus, if g is a primitive root modulo m, then

$$\prod_{x\in(\mathbb{Z}/m\mathbb{Z})^*} x = g^{\frac{m_1(m_1-1)}{2}} = g^{\frac{m_1}{2}} = -1.$$

Hence,

$$\prod_{x\in(\mathbb{Z}/m\mathbb{Z})^*} x = \begin{cases}-1 & \text{if } (\mathbb{Z}/m\mathbb{Z})^* \text{ is cyclic}\\ 1 & \text{else}\end{cases}$$

which is just the claim of Proposition 1. □

We see that the proof works not only with $(\mathbb{Z}/m\mathbb{Z})^*$ but with any finite abelian group G which can be written as a product of cyclic groups of even order. Therefore, we obtain the following generalisation:

Corollary 2. *Let $m_1, \ldots, m_k$ be positive integers and suppose that*

$$G \simeq \mathcal{C}_{m_1} \times \ldots \times \mathcal{C}_{m_k}$$

is a finite abelian group. Then

$$\prod_{x \in G} x \neq 1$$

holds if and only if at most one of the numbers $m_1, \ldots, m_k$ is even.