Proposition 12.1. Let R be a commutative ring with $1 \neq 0$ and let $U$ be the set of all units.

Then $U$ is a group under multiplication.

Proof. We first check that $U$ is closed under multiplication. Let $u_1$ and $u_2$ be units. Then we may find $v_1$ and $v_2$ such that $u_1v_1 = u_2v_2 = 1$. It follows that

$$(u_1u_2)(v_1v_2) = (u_1v_1)(u_2v_2) = 1.$$ 

Thus $u_1u_2$ is a unit and so $u_1u_2 \in U$. Therefore $U$ is closed under multiplication.

We check the axioms for a group. We have already checked there is a well-defined multiplication. By assumption multiplication is associative in $R$ and so it is associative in $U$. $1$ is a unit and so $1 \in U$ plays the role of the identity. If $u \in U$ is a unit then by assumption there is an element $v \in R$ such that $uv = 1$. But then $v$ is a unit so that $v \in U$ and $v$ is the inverse of $u$.

It follows that $U$ is a group. \qed

Theorem 12.2 (Fermat’s Little Theorem). If $a \in \mathbb{Z}$ is an integer then $a^p = a \mod p$.

In particular, if $a$ is coprime to $p$ then $a^{p-1} = 1 \mod p$.

Proof. Since $\mathbb{Z}_p$ is a field every non-zero element is a unit. $\mathbb{Z}_p$ has $p$ elements so that there are $p - 1$ units. Therefore every unit has order dividing $p - 1$, by Lagrange. In particular if $r$ is a non-zero element of $\mathbb{Z}_p$ then $r^{p-1} = 1$ in $\mathbb{Z}_p$.

If $a$ is coprime to $p$ then its remainder is a unit. Therefore $a^{p-1} = 1 \mod p$. This is the second statement.

Now suppose that $a$ is an arbitrary integer. If it is coprime to $p$ then

$$a^p = a^{p-1}a = 1a = a.$$ 

If it is not coprime to $p$ then the remainder is zero. As $0^p = 0$ we still have $a^p = a \mod p$. \qed

(12.2) is very useful.

Example 12.3. What is the remainder when you divide $26^{566}$ by $17$?

First note that $26$ has remainder $9$ when divided by $17$. So it suffices to compute $9^{566}$ modulo $17$. Now Fermat implies that

$$9^{16} = 1 \mod 17.$$ 

We can write

$$566 = 35 \cdot 16 + 6.$$ 

12. Fermat Theorem
Thus
\[26^{566} = 9^{566}\]
\[= 3^{35\cdot16+6}\]
\[= (9^{16})^{35} 9^6\]
\[= 9^6\]
\[= 3^{12}\]
\[= (3^3)^4\]
\[= (27)^4\]
\[= (10)^4\]
\[= (100)^2\]
\[= (-2)^2\]
\[= 4 \mod 17.\]

**Example 12.4.** Is \(2^{86,243} - 1\) divisible by 11?

As before, let’s compute the remainder of \(2^{86,243}\) after dividing by 11. By Fermat, if we raise 2 to a multiple of 10 then we get a remainder of 1,
\[2^{10} = 1 \mod 11.\]

Thus
\[2^{86,243} = 2^{86240+3}\]
\[= 2^{8624\cdot10+3}\]
\[= (2^{10})^{8624} 2^3\]
\[= 2^3\]
\[= 8 \neq 1 \mod 11.\]

Thus \(2^{86,243} - 1\) is not divisible by 11. In fact 86,243 is a prime number and it is known that \(2^{86,243} - 1\) is a prime number. Primes of the form \(2^p - 1\) where \(p\) is prime are known as Mersenne primes.

**Example 12.5.** Show that \(n^{49} - n\) is divisible by 15, for every integer \(n\).

As 3 and 5 are coprime, it is enough to check that \(n^{49} - n\) is divisible by 3 and 5. Note that \(n^{49} - n = n(n^{48} - 1)\).

If \(n\) is divisible by three then so is \(n^{49} - n\). Otherwise \(n\) is coprime to 3 and by Fermat
\[n^2 = 1 \mod 3.\]
Thus

\[ n^{48} = (n^2)^{24} \]
\[ = 1 \mod 3. \]

Thus 3 always divides \( n^{49} - n \).

If \( n \) is divisible by five then so is \( n^{49} - n \). Otherwise \( n \) is coprime to 5 and by Fermat

\[ n^4 = 1 \mod 5. \]

Thus

\[ n^{48} = (n^4)^{12} \]
\[ = 1 \mod 5. \]

Thus 5 always divides \( n^{49} - n \).

Hence 15 always divides \( n^{49} - n \).