4. Fermat–Euler Theorem

4.1 Reduced residue systems

Definition 4.1 A set $\{a_1, a_2, \ldots, a_h\}$ is called a *reduced residue system modulo* m, or a *reduced system modulo* m, if

(i) $a_i \not\equiv a_j \pmod{m}$ for any $i \neq j$;
(ii) $(a_i, m) = 1$ for $1 \leq i \leq h$;
(iii) For any integer a with $(a, m) = 1$, there exists an index i such that $a \equiv a_i \pmod{m}$.

Example 4.1 (i). $\{1, 5\}$ is a reduced system modulo 6; (ii). $\{1, 2, \ldots, p-1\}$ is a reduced system modulo p for p a prime.

Theorem 4.1 Let $\{a_1, \ldots, a_h\}$ be a reduced system modulo m and let k be an integer with $(k, m) = 1$. Then $\{ka_1, \ldots, ka_h\}$ is also a reduced system modulo m.

Proof. This proof is similar to that for Theorem 3.6.

(i). The same as Part (i) in the proof of Theorem 3.6.

(ii). Show $(ka_i, m) = 1$ for $1 \leq i \leq h$. Since k and a_i have no common divisors > 1 with m, so does their product ka_i.

(iii). Show $a \equiv ka_i \pmod{m}$ for some i for any a with $(a, m) = 1$. Since $(k, m) = 1$, we may find an integer k' with $kk' \equiv 1 \pmod{m}$. Note that $(k', m) = 1$ for if d is a common divisor of k' and m, then $d \mid (kk' - mx) = 1$ where x is such that $kk' - 1 = mx$. Thus, $(ak', m) = 1$. Choose i such that $a_i \equiv ak' \pmod{m}$. Then $ka_i \equiv k(ak') = a(kk') \equiv a \pmod{m}$. ∎

4.2 Euler's totient function

Note that a reduced system modulo m is a subset of a complete system modulo m. In particular, the size h of any reduced system modulo m equals the number of integers among $\{1, 2, \ldots, m\}$ that are coprime to m.

Definition 4.2 Let n be a positive integer. The *Euler totient function* $\phi(n)$ denotes the number of integers among $\{1, 2, \ldots, n\}$ that are coprime to n.

Example 4.2 (i). $\phi(1) = 1$ for 1 is the only integer in $\{1\}$ that is coprime to 1; (ii). $\phi(3) = 2$ for 1 and 2 are the integers in $\{1, 2, 3\}$ that are coprime to 3; (iii). $\phi(6) = 2$ for 1 and 5 are the integers in $\{1,2,3,4,5,6\}$ that are coprime to 6. ■

> **R** We may replace $\{1,2,\dots,n\}$ in the definition of Euler's totient function by any complete system modulo n.

Theorem 4.2 Let p be a prime and k be a positive integer. Then

$$\phi(p^k) = p^k - p^{k-1}. \tag{4.1}$$

Proof. Recall that $\phi(p^k)$ equals the number of integers in $\{1,\dots,p^k\}$ that are coprime to p^k, or in other words, that are not divisible by p. Since there are p^{k-1} integers among $\{1,\dots,p^k\}$ that are multiples of p, namely, $p\cdot 1$, $p\cdot 2$, $\dots$, $p\cdot p^{k-1}$, we have $\phi(p^k) = p^k - p^{k-1}$. ■

How to determine $\phi(n)$ if n is not a prime power?

Theorem 4.3 Let m and n be such that $(m,n)=1$. Then

$$\phi(mn) = \phi(m)\phi(n). \tag{4.2}$$

Proof. We have shown in Theorem 3.7 that $\{bm+an : 1\le a\le m, 1\le b\le n\}$ is a complete system modulo mn. Thus, to compute $\phi(mn)$, it suffices to count the number of such $bm+an$ with $(bm+an,mn)=1$. Note that

$$\begin{aligned}(bm+an,mn)=1 \quad &\Leftrightarrow \quad (bm+an,m)=1 \ \& \ (bm+an,n)=1\\ &\Leftrightarrow \quad (an,m)=1 \qquad\quad \& \ (bm,n)=1\\ &\Leftrightarrow \quad (a,m)=1 \qquad\quad\ \ \& \ (b,n)=1.\end{aligned}$$

Thus, there are $\phi(m)$ possibilities of a and $\phi(n)$ possibilities of b, and therefore $\phi(m)\phi(n)$ possibilities of admissible $bm+an$. It follows that $\phi(mn)=\phi(m)\phi(n)$. ■

> **R** Given an arithmetic function $f:\mathbb{Z}\to\mathbb{C}$, we say that it is *multiplicative* if for any m and n with $(m,n)=1$,
> $$f(mn) = f(m)f(n).$$

Corollary 4.4 For any integer $n\ge 2$,

$$\phi(n) = n\cdot\prod_{p\mid n}\left(1-\frac{1}{p}\right), \tag{4.3}$$

where the product runs over all prime divisors of n.

Proof. We write n in its canonical form $n=\prod_{i=1}^r p_i^{\alpha_i}$. Then by Theorem 4.3,

$$\phi(n) = \prod_{i=1}^r \phi(p_i^{\alpha_i}).$$

Further, making use of Theorem 4.2 gives

$$\prod_{i=1}^r \phi(p_i^{\alpha_i}) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^r p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = \prod_{i=1}^r p_i^{\alpha_i}\cdot\prod_{i=1}^r\left(1-\frac{1}{p_i}\right) = n\cdot\prod_{i=1}^r\left(1-\frac{1}{p_i}\right),$$

implying the desired result. ■

Theorem 4.5 Let n be a positive integer. Then

$$\sum_{d|n} \phi(n) = n,$$

where the sum runs over all divisors of n.

Proof. We write $n = \prod_{p|n} p^{\alpha}$. Then the divisors of n are of the form $\prod_{p|n} p^{\beta}$ with $0 \le \beta \le \alpha$ for each p. Thus,

$$\begin{aligned}\sum_{d|n} \phi(n) = \sum \phi\left(\prod_{\substack{p|n \\ 0\le\beta\le\alpha}} p^{\beta}\right) &= \sum \prod_{\substack{p|n \\ 0\le\beta\le\alpha}} \phi(p^{\beta}) \\ &= \prod_{p|n} \sum_{0\le\beta\le\alpha} \phi(p^{\beta}) = \prod_{p|n} \left(1 + (p-1) + (p^2 - p) + \cdots + (p^{\alpha} - p^{\alpha-1})\right) \\ &= \prod_{p|n} p^{\alpha} = n,\end{aligned}$$

giving the desired result. ■

R This relation gives an instance of the *Dirichlet convolution* that will be discussed in later lectures.

4.3 Fermat–Euler Theorem

Theorem 4.6 (Fermat–Euler Theorem). If $(a,m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{4.4}$$

Proof. Let $\{x_1, \ldots, x_{\phi(m)}\}$ be a reduced system modulo m. Thus, $(x_i, m) = 1$ for each i. Since $(a,m) = 1$, we know from Theorem 4.1 that $\{ax_1, \ldots ax_{\phi(m)}\}$ is also a reduced system modulo m. Thus,

$$\prod_{i=1}^{\phi(m)} x_i \equiv \prod_{i=1}^{\phi(m)} (ax_i) = a^{\phi(m)} \prod_{i=1}^{\phi(m)} x_i \pmod{m}.$$

Since $(x_i, m) = 1$ for each i, we have $(\prod_i x_i, m) = 1$. Thus, by Corollary 3.5, $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

The m equal to a prime p case is also known as *Fermat's Theorem*.

Corollary 4.7 (Fermat's Theorem). If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.5}$$

4.4 Binomial coefficients

Definition 4.3 For integers $m \ge n \ge 0$, the *binomial coefficients* are defined by

$$\binom{m}{n} = \frac{m!}{n!(m-n)!} = \frac{m(m-1)\cdots(m-n+1)}{n(n-1)\cdots 1}.$$

In particular, $\binom{m}{0} = 1$.

Theorem 4.8 (Pascal's identity). For integers $m \geq n > 0$,

$$\binom{m+1}{n} = \binom{m}{n} + \binom{m}{n-1}. \tag{4.6}$$

Proof. We have

$$\begin{aligned}
\binom{m}{n} + \binom{m}{n-1} &= \frac{m!}{n!(m-n)!} + \frac{m!}{(n-1)!(m-n+1)!} \\
&= \frac{m!}{(n-1)!(m-n)!} \cdot \frac{1}{n} + \frac{m!}{(n-1)!(m-n)!} \cdot \frac{1}{m-n+1} \\
&= \frac{m!}{(n-1)!(m-n)!} \cdot \frac{m+1}{n(m-n+1)} \\
&= \frac{(m+1)!}{(n)!(m-n+1)!},
\end{aligned}$$

which is exactly $\binom{m+1}{n}$. ■

Theorem 4.9 (Binomial Theorem). For $n \geq 1$,

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}. \tag{4.7}$$

Proof. We prove by induction on n. First, when $n = 1$, both sides of (4.7) are $x+y$. Assuming that (4.7) is true for some $n \geq 1$, we want to show that it is also true for $n+1$. Note that

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\left(\sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}\right) \\
&= \sum_{r=0}^{n} \binom{n}{r} x^{r+1} y^{n-r} + \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r+1} \\
&= \left(x^{n+1} + \sum_{r=0}^{n-1} \binom{n}{r} x^{r+1} y^{n-r}\right) + \left(y^{n+1} + \sum_{r=1}^{n} \binom{n}{r} x^r y^{n-r+1}\right) \\
&= \left(x^{n+1} + \sum_{r=1}^{n} \binom{n}{r-1} x^r y^{n-r+1}\right) + \left(y^{n+1} + \sum_{r=1}^{n} \binom{n}{r} x^r y^{n-r+1}\right) \\
&= x^{n+1} + y^{n+1} + \sum_{r=1}^{n} \left(\binom{n}{r-1} + \binom{n}{r}\right) x^r y^{n-r+1} \\
&= x^{n+1} + y^{n+1} + \sum_{r=1}^{n} \binom{n+1}{r} x^r y^{n-r+1} \\
&= \sum_{r=0}^{n+1} \binom{n+1}{r} x^r y^{n-r+1},
\end{aligned}$$

which is exactly the $n+1$ case of (4.7). ■

Corollary 4.10 The binomial coefficients $\binom{m}{n}$ are integers.

Theorem 4.11 Let p be a prime. Given any nonzero integer n, we denote by $\nu_p(n)$ the unique nonnegative integer k such that $p^k \mid n$ and $p^{k+1} \nmid n$, namely, $\nu_p(n)$ is the power of p in the canonical form of n. Let α be a positive integer. For $1 \le r \le p^\alpha$,

$$\nu_p\left(\binom{p^\alpha}{r}\right) = \alpha - \nu_p(r). \tag{4.8}$$

In particular, for any r with $1 \le r \le p-1$, we have $p \mid \binom{p}{r}$.

Proof. Recall that $\binom{p^\alpha}{r} = \frac{p^\alpha(p^\alpha-1)\cdots(p^\alpha-r+1)}{r(r-1)\cdots 1}$. For each s with $1 \le s \le r-1 < p^\alpha$, we observe the simple fact that $\nu_p(s) = \nu_p(p^\alpha - s)$. Hence, $\nu_p(\binom{p^\alpha}{r}) = \nu_p(p^\alpha) - \nu_p(r) = \alpha - \nu_p(r)$. ■

Theorem 4.11 has two important consequences.

Theorem 4.12 For $\alpha \ge 1$ and p prime, if

$$m \equiv 1 \pmod{p^\alpha},$$

then

$$m^p \equiv 1 \pmod{p^{\alpha+1}}.$$

Proof. We write $m = kp^\alpha + 1$ for a certain integer k. Then

$$m^p = (kp^\alpha + 1)^p = \sum_{r=0}^{p} \binom{p}{r} (kp^\alpha)^r = 1 + \sum_{r=1}^{p} \binom{p}{r} (kp^\alpha)^r.$$

Now, for $1 \le r \le p$, $\binom{p}{r} \cdot (p^\alpha)^r$ is always divisible by $p^{\alpha+1}$. ■

Theorem 4.13 For $k \ge 1$ and p prime,

$$(x_1 + x_2 + \cdots + x_k)^p \equiv x_1^p + x_2^p + \cdots x_k^p \pmod{p}. \tag{4.9}$$

Proof. We apply induction on k. The $k = 1$ case is trivial. Assume that the statement is true for some $k \ge 1$. Then we prove the $k+1$ case:

$$\begin{aligned}(x_1 + x_2 + \cdots + x_{k+1})^p &= \big(x_1 + (x_2 + \cdots + x_{k+1})\big)^p \\ &= \sum_{r=0}^{p} \binom{p}{r} x_1^r (x_2 + \cdots + x_{k+1})^{p-r} \\ &\equiv x_1^p + (x_2 + \cdots + x_{k+1})^p \\ &\equiv x_1^p + x_2^p + \cdots x_{k+1}^p \pmod{p},\end{aligned}$$

by our inductive assumption. ■

4.5 Euler's proof of the Fermat–Euler Theorem

We first prove that for $\alpha \ge 1$ and p prime, if a is such that $(a, p) = 1$,

$$a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}. \tag{4.10}$$

For its proof, we first choose $k=a$ in Theorem 4.13 and then put $x_1=\cdots=x_a=1$. Thus, $a^p\equiv a \pmod p$. Since $(a,p)=1$, we have $a^{p-1}\equiv 1 \pmod p$. Now, by an iterative application of Theorem 4.12, we have $a^{(p-1)p}\equiv 1 \pmod{p^2}$, ..., and $a^{(p-1)p^{\alpha-1}}\equiv 1 \pmod{p^\alpha}$, which is exactly (4.10).

Now, for integers m, we write $m=\prod_i p_i^{\alpha_i}$. Assume that a is such that $(a,m)=1$, and thus $(a,p_i)=1$ for each i. We also write for convenience $m=p_i^{\alpha_i}m_i$. Since ϕ is multiplicative, $\phi(m)=\phi(p_i^{\alpha_i})\phi(m_i)$. Thus, by (4.10),

$$a^{\phi(m)}=\left(a^{\phi(p_i^{\alpha_i})}\right)^{\phi(m_i)}\equiv 1^{\phi(m_i)}=1 \pmod{p_i^{\alpha_i}}.$$

That is, $a^{\phi(m)}-1$ is a multiple of each $p_i^{\alpha_i}$, and thus a multiple of $m=\prod_i p_i^{\alpha_i}$. In other words,

$$a^{\phi(m)}\equiv 1 \pmod m,$$

as desired.