Elementary Number Theory
Course I - High Diploma Students
Asst. Prof. Dr. Ruma Kareem K. Ajeena
ruma.usm@gmail.com

Mathematics Department
Edu. College for Pure Sciences
University of Babylon
2018-2019

Lecture 5: Fermat's Theorem

4.1 Fermat's theorem

Theorem 4.1.1. (Fermat's theorem). Let *p* be a prime and suppose that *p* is not divide *a*. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. The first $p-1$ positive multiples of a is the integers

$$a, 2a, 3a, ..., (p-1)a$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that $ra \equiv sa \pmod{p}$, $1 \leq r < s \leq p-1$ then $r \equiv s \pmod{p}$, which is impossible.

Therefore, the previous set of integers must be congruent modulo p to 1,2,3,...,p−1. Multiplying all these congruences together results

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

whence $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. By canceling $(p-1)!$ from both sides of the preceding congruence (since p is not divide $(p-1)!$), so $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.

Corollary 4.1.2. If p is a prime, then $a^{p} \equiv a \pmod{p}$ for any integer a.

Proof. H.W.

Fermat's theorem has many applications and solving some problems in number theory. For example, how to verify that

Dr. Ruma Kareem K. Ajeena

$$5^{38} \equiv 4(\text{mod}11).$$

One can know $5^{10} \equiv 1 \pmod{11}$ form (Fermat's theorem) and it can compute that as

$$5^{38} = 5^{10\cdot 3+8} = (5^{10})^3(5^2)^4 \equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Another use of Fermat's theorem is as a tool in testing the primality of a given integer *n*. If it could be shown that the congruence $a^n \equiv a \pmod{n}$ fails to hold for some choice of *a*, then *n* is necessarily composite.

As an example, if $n = 117$ and $a = 2$. Since 2^{117} can be written as

$2^{117} = 2^{7\cdot 16+5} = (2^7)^{16}\cdot 2^5$ and $2^7 = 128 \equiv 11 \pmod{117}$,

we have $2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 \cdot 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$. But $2^{21} = (2^7)^3$, which leads to $2^{21} \equiv 11^3 \equiv 121\cdot 11 \equiv 4\cdot 11 \equiv 44 \pmod{117}$. Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117},$$

so that 117 must be composite as 117=13·9.

Lemma 4.1.3. If *p* and *q* are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Proof. From corollary (4.1.2) tells us that $(a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p|a^{pq} - a$. In similar manner, $q|a^{pq} - a$. Corollary [If a|c and b|c, with gcd(a,b)=1, then ab|c] now yields $pq|a^{pq} - a$, which can be recast as $a^{pq} \equiv a \pmod{pq}$.

Example (converse to Fermat's theorem).
$2^{340} \equiv 1 \pmod{341}$, where $341 = 11\cdot 31$. Notice that $2^{10} = 1024 = 31\cdot 33+1$. Thus, $2^{11} = 2\cdot 2^{10} \equiv 2\cdot 1 \equiv 2 \pmod{31}$ and $2^{31} = 2(2^{10})^3 \equiv 2\cdot 1^3 \equiv 2 \pmod{11}$.
Exploiting the lemma, $211\cdot 31 \equiv 2 \pmod{11\cdot 31}$ or $2^{341} \equiv 2 \pmod{341}$. After canceling a factor of 2, we get to

$$2^{340} \equiv 1 \pmod{341}$$

so that the converse to Fermat's theorem is false.

Definition 4.1.5. (pseudoprime). A composite integer *n* is called

Dr. Rumi Kareem K. Ajeena

pseudoprime whenever $n|2^n - 2$.

In previous example, $341|2^{341} - 2$, although $341 = 11 \cdot 31$. The smallest four being 341, 561, 645, and 1105 and so on.

Definition 4.1.6 (pseudoprime to the base *a*). A composite integer n for which $a^n \equiv a \pmod{n}$ is called a pseudoprime to the base a.

When a =2, n is simply said to be a pseudoprime. For instance, 91 is the smallest pseudoprime to base 3, whereas 217 is the smallest such to base 5. It has been proved (in 1903) that there are infinitely many pseudoprimes to any given base.

The first example of an even pseudoprime, namely, the number $161038 = 2 \cdot 73 \cdot 1103$.

Note that: There exist composite numbers n which are pseudoprimes to every base a; that is, $a^{n-1} = 1 \pmod{n}$ for all integers a with $\gcd(a,n)=1$.

For example, the number 561. Please check that.
These exceptional numbers are called absolute pseudoprimes or Carmichael numbers.
To see that $561=3 \cdot 11 \cdot 17$ must be an absolute pseudoprime, notice that $\gcd(a,561)=1$ gives $\gcd(a,3)= \gcd(a,11)= \gcd(a,17)=1$.

An application of Fermat's theorem leads to the congruences

$$a^2 \equiv 1 \pmod{3} \quad a^{10} \equiv 1 \pmod{11} \quad a^{16} \equiv 1 \pmod{17}$$

and, in turn, to

$$a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3}$$
$$a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}$$
$$a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}$$

These give rise to the single congruence $a^{560} \equiv 1 \pmod{561}$, where $\gcd(a,561)=1$.
But then $a^{561} \equiv a \pmod{561}$ for all a, showing 561 to be an absolute pseudoprime.

Theorem 4.1.7 (Wilson). If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Dr. Ruma Kareem K. Ajeena

Example. A concrete example should explain to clarify the proof of Wilson's theorem.
Let p =13. It is possible to divide the integers 2,3,...,11 into (p−3)/2=5 pairs, each product of which is congruent to 1 modulo 13.

To write these congruences out explicitly:

$$2\cdot 7\equiv 1 \pmod{13}$$
$$3\cdot 9\equiv 1 \pmod{13}$$
$$4\cdot 10\equiv 1 \pmod{13}$$
$$5\cdot 8\equiv 1 \pmod{13}$$
$$6\cdot 11\equiv 1 \pmod{13}.$$

Multiplying these congruences gives the result

$$11!=(2\cdot 7)(3\cdot 9)(4\cdot 10)(5\cdot 8)(6\cdot 11)\equiv 1 \pmod{13}$$

and so

$$12!\equiv 12\equiv -1 \pmod{13}.$$

Thus, $(p-1)!\equiv -1 \pmod{p}$, with p =13.

Dr. Ruma Kareem K. Ajeena