Fermat's Theorem for Part IA Discrete Mathematics

Note This handout contains several exercises and past papers to the *Fermat's Little Theorem.* It also includes some optional material on its usage in primality testing and some on its extension, i.e. *Fermat-Euler's Theorem.*

Fermat's Theorem

Proof

Lemma 1. For all primes p, then $\binom{p}{0} \equiv 1 \pmod{p}$ and $\binom{p}{1} \equiv 1 \pmod{p}$.

Lemma 2. For all primes p and integers $0 < m < p$, then $\binom{p}{m} \equiv 0 \pmod{p}$.

Lemma 3 (The Freshman's Dream)**.** For all natural numbers m, n and primes p,

$$(m+n)^p \equiv m^p + n^p \pmod{p}.$$

Lemma 4 (The Dropout Lemma)**.** For all natural numbers m and primes p, $(m+1)^p \equiv m^p + 1 \pmod{p}$.

Lemma 5 (The many Dropout Lemma)**.** For all natural numbers m and i and primes p, $(m+i)^p \equiv m^p + i \pmod{p}$.

Theorem 1 (Fermat's Little Theorem (Part a))**.** For all natural numbers i and primes p, $i^p \equiv i \pmod{p}$.

Theorem 2 (Fermat's Little Theorem (Part b))**.** For all natural numbers i and primes p, if $p \nmid i$, then $i^{p-1} \equiv 1 \pmod{p}$.

(optional) An alternative proof

Theorem 3 (Fermat's Little Theorem (Part b))**.** For all natural numbers i and primes p, if $p \nmid i$, then $i^{p-1} \equiv 1 \pmod{p}$.

*Proof.*Consider the $p-1$ positive multiples of i, i.e.

$$i, 2i, 3i, \dots, (p-1)i$$

Since $\gcd(i, p) = 1$, this means that i has an inverse i^{-1} in $\mathbb{Z}_p$ (see the GCD handout). Hence,

$$i \cdot x \equiv i \cdot y \pmod{p} \Rightarrow i^{-1} \cdot i \cdot x \equiv i^{-1} \cdot i \cdot y \pmod{p} \Rightarrow x \equiv y \pmod{p}$$

Therefore all the multiples have to be different. Also, note that none of the $i \cdot x \equiv 0 \pmod{p}$, as this would imply that $p \mid i$ or $p \mid x$, which cannot be true by assumption. So, $i, 2i, 3i, \dots, (p-1)i$ is a permutation of $1, 2, 3, \dots, (p-1)$.

Now, we perform a tricky part. Multiply all the $i, 2i, 3i, \dots, (p-1)i$ together.

$$\begin{gathered}
i \cdot 2i \cdot 3i \cdot \ldots \cdot (p-1)i \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p} \Rightarrow \\
(1 \cdot 2 \cdot \ldots \cdot (p-1))\, i^{p-1} \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p} \Rightarrow \text{(By associativity)} \\
i^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p} \Rightarrow \text{(By factorial definition)} \\
i^{p-1} \equiv 1 \pmod{p} \ (\text{since} \gcd((p-1)!, p) = 1)
\end{gathered}$$

□

Further reading: There is also a proof using a combinatorial argument for counting necklaces consisting of beads of different colours. See the Christmas projects for more details.

Applications

Divisibility

Example 1. Find the remainder of 41^{75} when divided by 3.

*Proof.*By Fermat's theorem, we have since $\gcd(41, 3) = 1$, $41^2 \equiv 1 \pmod 3$. Hence, $41^{74} \equiv 1^{74} \pmod 3$ so $41^{74} \equiv 1 \pmod 3$. By noticing that $41 \equiv 2 \pmod 3$ and using the multiplication property of modulo, we get $41^{75} \equiv 2 \pmod 3$. Since $0 \leq 2 < 3$, the remainder is 2. □

Example 2. (Requires knowledge of Chinese Remainder Theorem) What is the last digit of 2^{400}?

*Proof.*By Fermat's theorem we have that $2^4 \equiv 1 \pmod 5$ so $2^{400} \equiv 1 \pmod 5$. We also know that $2^{400} \equiv 0 \pmod 2$, so the only number in $\mathbb{Z}_{10}$ that satisfies both of these modular equations is 6. Hence $2^{400} \equiv 6 \pmod{10}$.

(Alternative solution: Looking at the last digits for 2^i we get $2, 4, 8, 6, 2, 4, 8, 6, \ldots$. Hence, the values repeat every 4 multiplications, hence 2^{400} will have the same digit as $2^4 = 16$, so 6. □

Example 3. Let $p \neq q$ be two odd primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

*Proof.*By Fermat's theorem we have $p^{q-1} \equiv 1 \pmod q$ since $\gcd(p, q) = 1$. Similarly, $q^{p-1} \equiv 1 \pmod p$.

Hence, $q \mid p^{q-1} - 1$ and $p \mid q^{p-1} - 1$. Therefore, $pq \mid (p^{q-1} - 1)(q^{p-1} - 1)$ so $pq \mid p^{q-1}q^{p-1} - q^{p-1} - p^{q-1} - 1$ so $q^{p-1} - p^{q-1} \equiv 1 \pmod{pq}$. □

Lemma 6. If $a^k \equiv a \pmod m$ and $a^k \equiv a \pmod n$ for m, n co-prime, $a^k \equiv a \pmod{mn}$.

*Proof.*Note that $a^k \equiv a \pmod{m} \Rightarrow m \mid a^k - a$ and $a^k \equiv a \pmod{n} \Rightarrow n \mid a^k - a$. Since m and n are co=prime, Euclid's theorem implies that $nm \mid a^k - a$, i.e. $a^k \equiv a \pmod{mn}$. □

Example 4. Show that $a^{21} \equiv a \pmod{15}$ for all $a \in \mathbb{Z}$.

Proof.(Method 1) Since 5 is prime, by Fermat's Little Theorem, for a not a multiple of 5, $a^4 \equiv 1 \pmod{5}$. By the exponentiation property of modulo, $(a^4)^5 \equiv (1)^5 \pmod{5}$, so $a^{20} \equiv 1 \pmod{5}$, so $a^{21} \equiv a \pmod{5}$. Note that the last relation holds for a a multiple of 5. Hence, $a^{21} \equiv a \pmod{5}$ for any a.

Similarly, since 3 is prime and $21 = 2 \cdot 10 + 1$, we have that $a^{21} \equiv a \pmod{3}$.

Hence, $3 \mid (a^{21} - a)$ and $a \mid (a^{21} - a)$. Using Lemma 6, since 3 and 5 are co-prime, we get $a^{21} \equiv a \pmod{15}$.

(Method 2) Using FLT, for any a, $a^5 \equiv a \pmod{5}$ and so $a^{21} \equiv a \cdot (a^5)^4 \equiv a \cdot a^4 \equiv a^5 \equiv a \pmod{5}$.

Similarly, using FLT, for any a, $a^3 \equiv a \pmod{3}$ and so $a^{21} \equiv (a^3)^7 \equiv a^7 \equiv a^3 \cdot a^3 \cdot a \equiv a \cdot a \cdot a \equiv a^3 \equiv a \pmod{3}$. Hence, for the same reason as in the first method we get the desired result. □

Exercise 1. For all $a \in \mathbb{Z}$, $a^7 \equiv a \pmod{42}$.

Exercise 2. For all $a \in \mathbb{Z}$, $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$.

Exercise 3. For all $a \in \mathbb{Z}$, $a^9 \equiv a \pmod{30}$.

Exercise 4. For all $a \in \mathbb{Z}$, $a^5 \equiv a \pmod{30}$.

Exercise 5. Design an exercise like the above.

Exercise 6. Use Fermat's Little Theorem to verify that $17 \mid 11^{121} + 1$.

Exercise 7. For every $a \in \mathbb{Z}$ prove that a and a^5 have the same digit.

Exercise 8. Deduce that $17|(13^{16n+2} + 1)$ for $n \in \mathbb{Z}^+$

Exercise 9. Deduce that $13|(9^{12n+4} - 9)$ for $n \in \mathbb{Z}^+$

Exercise 10. Show that for p an odd prime:

(a)

$$\sum_{k=1}^{p-1} k^{p-1} \equiv -1 \pmod{p}$$

(b)

$$\sum_{k=1}^{p-1} k^p \equiv 0 \pmod{p}$$

Exercise 11. Let a and b be integers and p prime, with $a^p \equiv b^p \pmod{p}$. Show that $a^p \equiv b^p \pmod{p}$. [Hint: Show that $a \equiv b \pmod{p}$ and use the many dropout lemma]

Computation

Computing the inverse of an element

One of the applications of Fermat's Little Theorem is to compute the inverse of an element in $\mathbb{Z}_p$. In particular, consider $a \in \mathbb{Z}_p^*$, then $a^{p-1} \equiv 1 \pmod{p}$. By a simple manipulation, we get

$$a^{p-2} \cdot a \equiv 1 \pmod{p}$$

Since a has a unique inverse (see GCD handout), it follows that a^{p-2} is that inverse.

How would you compute this value? For exponentiating any number to a power k in $\mathbb{Z}_m$ we can use the modular exponentiation algorithm (essentially `npow` with the `mod` operation after every multiplication). This requires $O(\log(k))$ multiplications.

Example 5. Using Fermat's Little Theorem, solve $3x \equiv 4 \pmod{7}$.

*Proof.*The multiplicative inverse of 3 in $\mathbb{Z}_7$ is given by $\mathrm{rem}(3^5, 7) = 5$. Hence, $5 \cdot 3 \equiv 1 \pmod{7}$. By the multiplication properties of mod , we have

$$3x \equiv 4 \pmod{7} \Rightarrow (5 \cdot 3)x \equiv (5 \cdot 4) \pmod{7} \Rightarrow x \equiv 20 \pmod{7} \Rightarrow x \equiv 6 \pmod{7}.$$

Hence, the solutions are $x = 7k + 6$ for $k \in \mathbb{Z}$. □

Implementation Challenge: Implement an algorithm that finds the multiplicative inverse of a in $\mathbb{Z}_m$ using the modular exponentiation algorithm.

(grey area) Primality testing

Fermat's algorithm can be used to test whether a natural is a probable prime or a composite. For example, one might randomly pick $a \in \{2, 3, \ldots, n-2\}$ and check if $a^p \equiv a \pmod{p}$. If we find any a for which this is not the case, then it means that n is composite. Otherwise, even if for all values this is true, then we cannot deduce that a number is prime because the converse of Fermat's Little Theorem does not hold. In particular, there exist composite numbers n, called *Carmichael number*, such that $a^n \equiv a \pmod{n}$ for all $a < n$.

The smallest such number is $561 = 3 \cdot 11 \cdot 17$, which we will prove that it is Carmichael.

Example 6. Show that 561 is a Carmichael number.

*Proof.*Note that $561 = 3 \cdot 11 \cdot 17$. By Fermat's little theorem, for any a not a multiple of 17,

$$a^{16} \equiv 1 \pmod{17} \Rightarrow (a^{16})^{35} \equiv (1)^{35} \pmod{17} \Rightarrow a^{560} \equiv 1 \pmod{17}.$$

Hence, $a^{561} \equiv a \pmod{17}$ (and this holds also for multiples of 17). Similarly, since $560 = 2{\cdot}280$ and $560 = 10{\cdot}56$, $a^{561} \equiv a \pmod{3}$ and $a^{561} \equiv a \pmod{11}$ hold respectively.

By the Lemma 6, since 3, 11 and 17 are co-prime, $a^{561} \equiv a \pmod{561}$, so 561 is a Carmichael number. □

Implementation challenge: Write a program to find as many of the 43 Carmichael numbers under one million.

A related notion is that of a *pseudo-prime*, which is a natural m such that $2^m \equiv 2$ for m not prime. In 2006P2Q3 you will prove that there is an infinite number of pseudoprimes.

Further reading: In practice, because of the existence of counterexamples, Fermat's Little Theorem is used as a subcomponent in more complicated primality test algorithms such as the Miller-Rabin, and Solovay-Strassen. The success rate of Fermat's primality test depends on the number of Carmichael numbers and on the proportion of $a \in \mathbb{Z}_n$ that satisfy $a^n \equiv a$ for a composite number n. In 1994, it was proven that the there exists an infinite number of Carmichael numbers along with a lower bound of at least $n^{2/7}$ such numbers below n. In the project questions, you can explore Erdős' proof for an upper bound.

Exercise 12. Show that for a Carmichael number n there cannot exist $k > 1$ such that $k^2 \mid n$.

Exercise 13. Let n be a composite square-free natural (i.e. not divisible by any square except for 1), say $n = p_1 p_2 \dots p_k$, where p_i are distinct primes. Show that if $p_i - 1 \mid n - 1$, then n is a Carmichael number. Why does this not imply the existence of infinitely many Carmichael numbers?

Exercise 14. Show that $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number.

Exercise 15. Show that $2821 = 7 \cdot 13 \cdot 31$ is a Carmichael number.

Exercise 16. Show that $561 \mid 2^{561} - 1$ and $561 \mid 3^{561} - 3$.

Note: It is an open question (according to "Elementary Number Theory" by D. M. Burton) if there exist infinitely many composite numbers n such that $n \mid 2^n - 2$ and $n \mid 3^n - 3$.

Past papers

COMPUTER SCIENCE TRIPOS Part IA – 2014 – Paper 2

7 Discrete Mathematics (MPF)

(*b*) (*i*) State Fermat's Little Theorem. [2 marks]

(*ii*) Prove that for all natural numbers m and n, and for all prime numbers p, if $m \equiv n \big(\mathrm{mod}\ (p-1)\big)$ then $\forall\, k \in \mathbb{N}.\, k^m \equiv k^n \pmod{p}$. [6 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2006 – Paper 2

3 Discrete Mathematics I (MPF)

(*a*) State Fermat's Little theorem, carefully defining any terms that you use. Deduce that $2^p \equiv 2 \pmod{p}$ for any prime p. [5 marks]

(b) Explain how this result can be used to show that a number is composite without actually finding a factor. Give an example. [3 marks]

(c) Let $M_m = 2^m - 1$ be the m^{th} Mersenne number. Suppose that m is composite. Prove that M_m is composite. [3 marks]

(d) A composite number m that satisfies $2^m \equiv 2 \pmod{m}$ is known as a *pseudo-prime.*

(i) Suppose that m is prime. Prove that M_m is either prime or a pseudo-prime. [3 marks]

(ii) Suppose that m is a pseudo-prime. Prove that M_m is a pseudo-prime. [3 marks]

(iii) Deduce that there are infinitely many pseudo-primes. [3 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2005 – Paper 1

2 Discrete Mathematics I (MPF)

(*a*) State the Fermat–Euler theorem, and deduce that $p \mid (2^p - 2)$ for any prime p. [5 marks]

(*b*) A composite number m that satisfies $m \mid (2^m - 2)$ is known as a *pseudo-prime*.

Show that $2^{10} \equiv 1 \pmod{11}$ and $2^{10} \equiv 1 \pmod{31}$. Deduce that 341 is a pseudo-prime. [5 marks]

COMPUTER SCIENCE TRIPOS Part IA – 1999 – Paper 1

8 Discrete Mathematics (MPF)

State and prove Fermat's Little Theorem. [8 marks]

Given a prime, p, with $p \neq 2$ and $p \neq 5$, show that there are infinitely many natural numbers, each of which has 9s as all its digits and which is divisible by p. [8 marks]

(optional) Euler-Fermat's Theorem

In this section, we are going to discuss Euler's generalisation of Fermat's Little Theorem. This theorem was taught in past versions of this course and has deep connections to many concepts/exercises in the current version of the course. So, if you have time it might be useful to learn about it (it will also come up in Part II Cryptography).

We begin with the definition for Euler's totient function.

Definition 1. For $n \in \mathbb{N}$ we define Euler's totient function $\phi(n)$ to be equal to the number of natural numbers $k \in \mathbb{Z}_n$ such that $\gcd(k, n) = 1$.

For example, $\phi(10) = 4$ since there are 4 numbers co-prime to 10 namely $1, 3, 7, 9$. We can prove the following trivial property.

Property 1. For any prime $p \in \mathbb{N}$, $\phi(p) = p - 1$.

*Proof.*Let $n \in \mathbb{Z}_p$, then $\gcd(n, p) = 1$. Since there are $p - 1$ of these $\phi(p) = p - 1$

For completeness we will also prove that $\gcd(n, p) = 1$ consider $d > 0$ such that $d \mid n$ and $d \mid p$, then since p is prime $d = 1$ or $d = p$.

However, $n < p$ so $d = 1$. So, any common divisor is 1, hence $\gcd(n, p) = 1$. □

Now, we are ready to state the Euler's extension of Fermat's little theorem.

Theorem 4. Let $n \in \mathbb{N}$ and $a \in \mathbb{N}$ with $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv a \pmod{n}.$$

Note: For n being a prime number this is Fermat's Little Theorem.

*Proof.*Consider $r_1, \ldots, r_{\phi(n)}$ to be the $\phi(n)$ numbers in $\mathbb{Z}_n$ co-prime with n. We will use the fact that for $a \in \mathbb{Z}_n$ and $\gcd(a, n) = 1$, a has an inverse $a^{-1} \in \mathbb{Z}_n$(see the GCD handout), meaning that $ar_i \equiv ar_j \pmod{n} \Rightarrow r_i \equiv r_j \pmod{n}$ (cancellation law).

So consider the values $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}$. Being the product to two values co-prime to n, their product will be co-prime with n, so one of the r_j values. By the cancellation law, no two of these can map to the same r_j. Hence, these $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}$ are a permutation of $r_1, r_2, \ldots, r_{\phi(n)}$.

Now, we will use a trick. Multiplying all the $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}$ together we get

$$\begin{aligned} a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv & \pmod{n} \Rightarrow \\ a^{\phi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv & \pmod{n} \Rightarrow \\ a^{\phi(n)} \equiv 1 & \pmod{n} \end{aligned}$$

where the last step follows from the fact that $r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)}$ is co-prime with n (as the product of values co-prime to n), so it must have an inverse. □

Properties of the ϕ function

Property 2. Let p be a prime and let $a \in \mathbb{N}$ for $a \geq 1$, then

$$\phi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$$

*Proof.*Let's count the values in $\mathbb{Z}_{p^a}$ that are not co-prime with p^a. If $\gcd(n, p^a) > 1$, then $\gcd(n, p) = p^k$ for some $k \in \mathbb{N}^*$. Hence, we are searching for the multiples of p, i.e. $p, 2p, 3p, \ldots, p^{a-1}, p^a$. There are $p^a/p = p^{a-1}$ of these. Therefore, the number of values co-prime with p^a are $\phi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$. □

Property 3. Let $a, b \in \mathbb{N}$ be positive with $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a) \cdot \phi(b)$.

*Proof.*This proof requires knowledge of the Chinese Remainder Theorem.

Consider the $\phi(a)$ values that are co-prime with a, $r_1^a, \ldots, r_{\phi(a)}^a$ and similarly $r_1^b, \ldots, r_{\phi(b)}^b$. An integer n will be co-prime with ab iff it is co-prime with both a and b. A integer n is co-prime with a iff $n \equiv r_i^a \pmod{a}$ for some i. So the values n co-prime to ab will be $n \equiv r_i^a \mod a$ and $n \equiv r_j^b \pmod{b}$ for some i, j.

By the Chinese remainder there is a one-to-one mapping between the pairs of modulo for a and b and the modulo for ab, hence, there must be $\phi(a) \cdot \phi(b)$ values (i.e. all possible (r_i^a, r_j^b) pairs) that are co-prime with ab. □

Property 4. For natural $n \geq 2$, $\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \left(1 - \frac{1}{p_k}\right)$, where p_i are the distinct primes that divide n.

*Proof.*By the fundamental theorem of arithmetic we have that $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ for $a_i \geq 0$. Note that $\gcd(p_i^{a_i}, p_j^{a_j}) = 1$, hence

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}) \\
&= \phi(p_1^{a_1}) \cdot \ldots \cdot \phi(p_k^{a_k}) \text{(by Property 3)} \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \text{(by Property 2)} \\
&= p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \text{(by re-arrangement)} \\
&= n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

□

Now, we have a simple way to compute the $\phi(n)$ given the factorisation of n.

For example, $\phi(10) = 10 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 4$ or $\phi(20) = \phi(5 \cdot 2^2) = 20 \cdot (1 - \frac{1}{5})(1 - \frac{1}{2}) = 8$.

Examples (under construction!)

Example 7. (Requires knowledge of the Chinese Remainder Theorem) Find the last two digits of 3^{400}.

*Proof.*We want to determine the remainder of 3^{400} when divided by 100, i.e. by $5^2 \cdot 2^2$. Note that $\phi(25) = 20$ and $\phi(4) = 1$. By Euler-Fermat's theorem, $3^{20} \equiv 1 \pmod{25}$ so $3^{400} \equiv 1 \mod 25$ and $3^2 \equiv 1 \pmod 4$ so $3^{400} \equiv 1 \pmod 4$. Hence, using the Chinese Remainder Theorem since $\gcd(4, 100) = 1$, $3^{400} \equiv 1 \pmod{100}$ and so the last two digits are 01. □

Past papers

COMPUTER SCIENCE TRIPOS Part IA – 2002 – Paper 1

7 Discrete Mathematics I (MPF)

(*a*) State carefully the Fermat–Euler theorem, defining any terms that you use. [4 marks]

(*b*) Explain how calculating a^{n-1}(mod n) for various values of a can be used to show that n is composite without actually finding its factors. By considering $561 = 3 \times 11 \times 17$ or otherwise, show that the test is not perfect and suggest an improvement to make it more selective. [6 marks]