Chapter 6

Prime Numbers

Prime numbers have been one of the most remarkable objects in mathematics since Euclid proved that there is an unending sequence of primes. In this Chapter, most of the results and methods that we have obtained so far come together to reveal the theory of primes.

Definition and Fundamental Results

Definition (prime number, composite number)**.** An integer p is **prime** if $p > 1$ and p has exactly two positive divisors, 1 and p.

If $n > 1$ and n is not prime, n is said to be **composite**.

The integer 1 is neither prime nor composite.

Lemma 6.1 (the form of composite numbers)**.** An integer n is composite if, and only if, $n = ab$ for some integers a, b with $1 < a, b < n$.

Proof. If $n = ab$ where $a, b > 1$, then $n > 1$ and n is not prime since a is a positive divisor if n which is neither 1 nor n. Hence by definition, n is composite.

Vice versa, if n is composite, then by definition $n > 1$ and n has a positive divisor a other than 1 and n; this means that $1 < a < n$ and that $n = ab$ with $b = n/a$. It remains to observe that $1 < b < n$. □

Example. The first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

Remark (Large primes)**.** It is a hard problem to prove that a given large integer (say with 150 digits) is prime. But some very large primes are known, such as $2^{82,589,933} - 1$ with more than 24 million decimal digits, found in December 2018 by the Great Internet Mersenne Prime Search. At the time of its discovery, this was the largest known prime number.

Question. What is the connection with the earlier definition of *coprime*?

Lemma 6.2 (divisor-coprime dichotomy)**.** If p is prime, then for all integers a, either $p \mid a$ or p and a are coprime.

Proof. Let p be a prime and a be an integer. We assume that $p \nmid a$ and prove that p is coprime to a. The only positive divisors of p are 1 and p. Out of these, p is not a divisor of a by assumption, so 1 is the only *common* positive divisor of p and a. Hence $\gcd(p, a) = 1$, so p is coprime to a by definition of "coprime". □

Proposition 6.3. Every integer $n \geq 2$ is a product of primes.

(With the convention that a product can be of just one prime!)

Proof. We prove this by *strong* induction.

Base case: $n = 2$ which is a product of one prime.

Inductive step: Assume that for all n such that $2 \leq n \leq k$, n is a product of primes. Our goal is to prove that $k + 1$ is a product of primes.

Since $k+1 > 1$, either $k+1$ is a prime — then it is a product of one prime, or $k+1$ is composite — then by Lemma 6.1, $k + 1$ is of the form ab with $2 \leq a, b \leq k$. By the Inductive Hypothesis, a, b are products of primes, hence $k + 1 = ab$ is also a product of primes.

Conclusion: by strong induction, every integer $n \geq 2$ is a product of primes. □

Theorem 6.4 (Euclid's property of a prime)**.** If p is a prime, then for all integers a, b, if p divides ab then $p \mid a$ or $p \mid b$.

Proof. Let p be a prime. Assume for contradiction that the statement of the Theorem is false; that is, there exist integers a, b such that $p \mid ab$ and $p \nmid a$ and $p \nmid b$.

Since $p \nmid a$, by Lemma 6.2 p is coprime to a.

Then since $p \mid ab$ and p is coprime to a, by the Coprime factor Lemma 2.4 $p \mid b$.

This contradicts the assumption $p \nmid b$. The contradiction shows that the statement of the Theorem was true. □

Remark. Euclid's property of a prime motivates the definition of a prime in more advanced work.

Example. 6 is not prime, because 6 has positive divisors $2, 3$ which are neither 1 nor 6.

Another way to prove that 6 is not prime would be to show that 6 does not possess Euclid's property of a prime. For example, $6 \mid 24$, yet $24 = 3 \times 8$ and $6 \nmid 3$ and $6 \nmid 8$; hence by Theorem 6.4, 6 is not prime.

Corollary 6.5 (Euclid's property of a prime for a product of n factors)**.** If a prime p divides the product $a_1a_2 \dots a_n$ of integers $a_1, \dots, a_n$, then $p \mid a_i$ for some $1 \le i \le n$.

Proof. Induction in n. Base case, $n = 2$, is Theorem 6.4.

Inductive step: let the statement be true for $n = k$; we prove it for $n = k + 1$. Assume that p divides $a_1a_2 \dots a_{k+1}$; write this as the product $(a_1a_2 \dots a_k) \times a_{k+1}$ of two factors. By Theorem 6.4,

- either $p \mid (a_1a_2 \dots a_k)$; then by the inductive hypothesis, $p \mid a_i$ for some $1 \le i \le k$;
- or $p \mid a_{k+1}$, that is, $p \mid a_i$ for $i = k + 1$.

In all cases the statement holds for $n = k+1$. By induction, the statement is true for all $n \ge 2$. □

Now we can prove that the product of primes guaranteed by Proposition 6.3 is unique (up to ordering).

Theorem 6.6 (Fundamental Theorem of Arithmetic)**.** Every integer greater than 1 can be written as a product of primes unique up to ordering, i.e. for all $n \ge 2$ there exist unique r and unique primes $p_1 \le p_2 \le \dots \le p_r$ such that

$$n = p_1p_2 \dots p_r.$$

Proof. Existence of prime factorisation is by Proposition 6.3. To prove uniqueness, assume for contradiction that two different products of primes give the same result. Cancel all primes which appear in both products, obtaining

$$p_1p_2 \dots p_r = q_1q_2 \dots q_s \quad \text{where} \quad p_i \ne q_j \quad \text{for all } i, j. \tag{*}$$

Note that $r, s > 0$, i.e., there is at least one prime on each side of this equation, because a product of primes cannot be equal to 1. Then $p_1 \mid q_1q_2 \dots q_s$ so by Corollary 6.5 $p_1 \mid q_j$ for some j. But since q_j is prime, the only divisor of q_j greater than one is q_j. So $p_1 = q_j$, contradicting (*). □

Primality testing I (how to check if n is a prime number?)

From the definition of a prime number, it may appear that we have to check each number from 2 to $n-1$ to see if it is a divisor of n. The process is made more efficient by the following result.

Proposition 6.7. If m is composite then m has a prime divisor not greater than $\sqrt{m}$.

Proof. Let $m = p_1 p_2 \dots p_r$ be the prime factorisation of m with $p_1 \le p_2 \le \cdots \le p_r$. Note that $r \ge 2$ since m is not a prime. Then $m \ge p_1 p_1 \dots p_1 = p_1^r \ge p_1^2$. Hence $\sqrt{m} \ge p_1$. □

The following method will test whether N is prime, and will generate all the prime numbers between 1 and N.

Algorithm (Sieve of Erathosthenes). • Write out the list of natural numbers from 2 up to N.

- Strike out all multiples of 2, except for 2 itself.
- Strike out all multiples of the next remaining number except that number itself (this will be 3).
- Continue, at each step striking out all multiples of the next remaining number except that number itself.
- Stop when the next remaining number is greater than $\sqrt{N}$.

Remark (Explanation why the Sieve of Eratosthenes works). Since we are striking out multiples we are **only** striking out composite numbers. Since every composite number $m \le N$ has, by Proposition 6.7, a (prime) divisor $\le \sqrt{m} \le \sqrt{N}$, we will strike out **every** composite number $\le N$. Thus what will remain will be the non-composite numbers, i.e. the primes, between 2 and N.

Example (sieve for primes up to 48). Write down the integers from 2 to 48.

		$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	**7**	~~8~~	~~9~~
~~10~~	**11**	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**
~~20~~	~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**
~~30~~	**31**	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~
~~40~~	**41**	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	

1. Mark $\mathbf{2}$ as a prime. Strike out every second number after 2: $\cancel{4}$, $\cancel{6}$ etc.

2. Mark the next remaining number $\mathbf{3}$ as a prime. Strike out every third number after 3: $\bcancel{6}$, $\bcancel{9}$ etc.

3. Mark the next remaining number $\mathbf{5}$ as a prime. Strike out every fifth number after 5: ~~10~~, ~~15~~ etc.

The next remaining number, 7, is greater than $\sqrt{48}$ so we stop. The numbers which we did not strike out are all the primes up to 48.

How many primes are there?

Euclid was probably the first to prove, in his *Elements*, the following statement.

Theorem 6.8. There are infinitely many primes.

Proof. Assume for contradiction that there are finitely many primes, and list all primes as $p_1, \ldots, p_r$. Let $N = p_1 p_2 \ldots p_r + 1$. Observe that N is not divisible by any prime, since N leaves remainder 1 when divided by p_i for all i. Yet by the Fundamental Theorem of Arithmetic, N must be divisible by a prime. This contradiction shows that the assumption that there are finitely many primes was false. Hence there are infinitely many primes. □

Remark. It needs to be stressed that this N may well **not** be prime. The first few N are

$$\begin{aligned}
&N = 2 + 1 = 3, && \text{prime,}\\
&N = 2 \times 3 + 1 = 7, && \text{prime,}\\
&N = 2 \times 3 \times 5 + 1 = 31, && \text{prime,}\\
&N = 2 \times 3 \times 5 \times 7 + 1 = 211, && \text{prime,}\\
&N = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311, && \text{prime,}\\
&N = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509 && \text{composite.}
\end{aligned}$$

The point of the proof is that the *prime divisors* of N will be previously unseen primes.

Fermat's Little Theorem and applications

Lemma 6.9 (binomial coefficients $\dbinom{p}{r}$, apart from the extreme ones, are divisible by prime p)**.** If p is prime then p divides the binomial coefficient $\dbinom{p}{r}$ for $1 \le r \le p - 1$.

Proof. Observe that, whenever r is between 1 and $p-1$,

$$r\binom{p}{r} = p\binom{p-1}{r-1}.$$

Indeed, by the Factorial Formula for the binomial coefficient, this translates as $\dfrac{r \times p!}{(p-r)!\,r!} = \dfrac{p \times (p-1)!}{(p-r)!\,(r-1)!}$ which is true. Hence p divides $r\binom{p}{r}$. But p does not divide r since $1 \leq r < p$, so by Euclid's property of a prime (Theorem 6.4), p divides $\binom{p}{r}$. □

Proposition 6.10 (Freshman's Dream)**.** For all $a, b \in \mathbb{Z}$ and all primes p we have

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Proof. By the Binomial Theorem, $(a+b)^p - (a^p + b^p) = \displaystyle\sum_{r=1}^{p-1} \binom{p}{r} a^{p-r} b^r$. By Lemma 6.9, p divides every term on the right, hence p divides the whole sum, hence $p \mid (a+b)^p - (a^p + b^p)$ as required. □

We are ready to prove the following famous result.

Theorem 6.11 (Fermat's Little Theorem)**.** For all $n \in \mathbb{Z}$, and all primes p,

$$n^p \equiv n \mod p, \qquad \text{and} \qquad \big(p \nmid n \implies n^{p-1} \equiv 1 \mod p\big).$$

Proof. Fix a prime p. We first prove that $n^p \equiv n \mod p$ **for non-negative** n by induction in n.

Base case: $n = 0$, $0^p \equiv 0$ trivially.

Inductive step: assume that $k^p \equiv k \mod p$. We need to prove $(k+1)^p \equiv k+1$.

Indeed, by Freshman's Dream, $(k+1)^p \equiv k^p + 1 \mod p$. By inductive hypothesis, $k^p \equiv k$ so $k^p + 1 \equiv k + 1 \mod p$ as required.

Conclusion: by induction $n^p \equiv n \mod p$ for all $n \geq 0$.

Proof for all $n \in \mathbb{Z}$**:** let now $n < 0$ and let r be a non-negative residue of n mod p (for example, the remainder) so that $r \equiv n \mod p$. By Modular Arithmetic $n^p \equiv r^p$ and by the proof above, $r^p \equiv r \mod p$. We have $n^p \equiv r^p \equiv r \equiv n$ so $n^p \equiv n \mod p$ as required.

Proof of the second statement of the theorem: assume that $p \nmid n$, then by Lemma 6.2, n is coprime to p. Take the already proved congruence $n^p \equiv n \mod p$ and divide both sides by the integer n, coprime to the modulus (Proposition 3.3). Obtain $n^{p-1} \equiv 1 \mod p$ as required. □

We present several applications of Fermat's Little Theorem.

Application: Calculating powers

Fermat's Little Theorem (FLT) can be used to calculate the remainder of a large power a^N of $a \in \mathbb{Z}$ when divided by a prime p. In Chapter 3 we used the Method of Successive Squaring for this purpose. Let us redo one of the examples using FLT:

Example. What is the remainder of 4^{100} when divided by 13?

Solution. Since 13 is a prime which does not divide 4, by FLT $4^{12} \equiv 1 \mod 13$. Thus

$$4^{100} = 4^{12\times 8+4} \equiv \left(4^{12}\right)^8 \left(4^2\right)^2 \equiv 1^{12} \left(-3\right)^2 \equiv 9 \mod 13,$$

(note how we wrote $100 = 12 \times 8 + 4$, i.e., we divided the exponent, 100, $12 = p - 1$, and found the remainder, 4). This reproduces the answer obtained in Chapter 3 with less effort.

Application: Finding and using inverses

If a is invertible mod p then by FLT $a^{p-1} \equiv 1 \mod p$, or equivalently $a^{p-2} \times a \equiv 1 \mod p$. This means that a^{p-2} is the inverse of a modulo p or, in the language of congruence classes,

$$[a]_p^{-1} = [a^{p-2}]_p \qquad \text{in} \quad \mathbb{Z}_p^*.$$

Remark (Efficiency of inverting a mod p using this method)**.** An interesting question is with which method is it quickest to calculate the inverse of an integer modulo a large prime. Is it by Euclid's Algorithm or by calculating a^{p-2} using, for example, the method of successive squaring?

In fact, both methods have running time proportional to the number of decimal digits of p. For Euclid's algorithm this result on the running time is Lamé's Theorem, see PJE p.226.

We have seen before that a use of inverses is to solve linear congruences.

Example. Invert 5 mod 19. Hence solve the congruence $5x \equiv 6 \mod 19$.

Solution. 19 is prime so Fermat's Little theorem implies $5^{18} \equiv 1 \mod 19$, so 5^{17} is the inverse of 5 mod 19.

Though this is **an** answer to the question, for practical purposes we normally look for the *least positive residue*. Successive squaring gives

$$5^2 \equiv 6, \quad 5^4 \equiv 17, \quad 5^8 \equiv 4, \quad 5^{16} \equiv 16 \qquad \text{so} \qquad 5^{17} \equiv 5 \times 16 \equiv 4 \mod 19.$$

Thus

$$5x \equiv 6 \iff 4 \times 5x \equiv 4 \times 6 \equiv 5 \iff x \equiv 5 \mod 19.$$

which *should still be checked by substitution*.

Remark. Fermat's Little Theorem may appear wonderful in that it helps us solve congruences and simplifies substantially the calculation of large powers modulo p. But the result has one weakness, you need to know that the modulus is prime. It should be stressed that **it is a difficult problem showing that a large number is prime (primality testing).**

Application: Primality Testing II: Fermat pseudoprime test

Testing whether n is a prime using *Sieve of Eratosthenes* may cost up to $\sqrt{n}$ operations. This is unacceptably slow in modern applications.

Modern methods use ideas around the following **Fermat pseudoprime test**, but unfortunately it is randomised and may give a "false prime" with non-zero probability:

- Pick a random integer a between 2 and $\sqrt{n}$;
- use Euclid's algorithm to find $d = \gcd(a, n)$. If $d > 1$, n is composite (divisible by d) and we are done;
- otherwise, calculate a^{n-1} mod n using successive squaring;
- if $a^{n-1} \not\equiv 1 \mod n$, then by Fermat's Little Theorem n is not prime.

Unfortunately, if we discover that $a^{n-1} \equiv 1$ mod n, we will not know if n is prime or composite. Indeed, $a^{n-1} \equiv 1$ mod n holds for all prime n but holds also for some composite n and some a coprime to n.

The number of steps in Euclid's Algorithm and successive squaring is only of order $\log n$ which is much smaller than $\sqrt{n}$. But it can happen that, even after picking several a, no contradiction is found, but n is still composite.

Euler's phi-function and Euler's Theorem

Recall from the previous chapter that $\mathbb{Z}_n^*$ is the set of invertible classes in $\mathbb{Z}_n$ and that it can be written as

$$\{[r]_n : 0 \le r \le n-1,\ \gcd(r,n) = 1\}\,.$$

Definition. Euler's phi-function is $\phi\colon \mathbb{N} \to \mathbb{N}$ given, for all $n \ge 1$, by

$$\begin{aligned}\phi(n) &= |\mathbb{Z}_n^*| \\ &= |\{r : 0 \le r \le n-1,\ \gcd(r,n) = 1\}|\,.\end{aligned}$$

Example.

- Simply by checking we see that $\phi(5) = 4$ and $\phi(7) = 6$.
- In general $\phi(p) = p - 1$ for all primes p since all positive integers strictly less than p are coprime to p by Lemma 6.2.
- Also by checking, we find that $\phi(8) = 4$ and $\phi(16) = 8$. In general $\phi(2^n) = 2^{n-1}$ for all $n \geq 1$, since in these cases we are counting the integers coprime to 2^n, i.e. the odd integers. And half of the integers up to 2^n are odd.
- And you can easily check by hand that $\phi(6) = 2$, $\phi(9) = 6$ and $\phi(10) = 4$.

Proposition 6.12 (rules for calculating $\phi(n)$)**.** a) If p is prime then for all $r \geq 1$

$$\phi(p^r) = p^{r-1}(p-1).$$

b) **Multiplicativity of ϕ:** If $\gcd(m, n) = 1$ then

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

Proof. a) We claim that the numbers **not coprime** to p^r are multiples of p. Indeed, if x is not coprime to p^r, that is, $\gcd(x, p^r) > 1$, then $\gcd(x, p^r)$ is divisible by a prime, but the only prime which divides p^r is p, hence $p \mid x$. Vice versa, if $p \mid x$ then x is not coprime to p^r.

Among the first p^r non-negative integers there are $\frac{p^r}{p}$ integers divisible by p, therefore

$$\phi(p^r) = |\{0, 1, \dots, p^r - 1\} \setminus \{x : \gcd(x, p^r) > 1\}| = p^r - |\{0, p, 2p, \dots\}| = p^r - p^{r-1}.$$

b) *Multiplicativity of ϕ is not proved in the lectures.*

We give an idea of proof which is **not** examinable. Assume that m and n are coprime. If x is a number between 0 and $mn - 1$ we denote

$$f(x) = ([x]_m, [x]_n) \quad \in \mathbb{Z}_m \times \mathbb{Z}_n.$$

This rule defines a function $f \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. By the Chinese Remainder Theorem this function is surjective: indeed, for any pair (c_1, c_2) where c_1 is a remainder mod m and c_2 is a remainder mod n, the Chinese Remainder Theorem gives some x_0, $0 \leq x_0 \leq mn - 1$, such that $f(x_0) = (c_1, c_2)$.

Since the function f is surjective and the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have the same cardinality mn, the function f is bijective.

One then checks that $[x]_{mn}$ is invertible mod mn if, and only if, $[x]_m$ is invertible mod m and $[x]_n$ is invertible mod n. Thus f gives a bijection between the sets $\mathbb{Z}_{mn}^*$ and $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. These two sets therefore have the same cardinality. Since, by definition, the cardinality of $\mathbb{Z}_n^*$ is $\phi(n)$ for all n, we have $\phi(mn) = \phi(m) \times \phi(n)$.

Note that we need m, n to be coprime to apply the Chinese Remainder Theorem in this argument. The equation $\phi(mn) = \phi(m)\phi(n)$ does not hold unless m, n are coprime. □

Corollary (formula for $\phi(n)$)**.** If $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s} = \prod_{i=1}^{s} p_i^{k_i}$ is the prime factorisation of n, where $p_1, \dots, p_s$ are distinct primes, then

$$\phi(n) = \prod_{i=1}^{s} p_i^{k_i - 1}(p_i - 1).$$

Proof. If $s = 1$, this is just part a) of the Proposition. Otherwise, $p_1^{k_1}$ is coprime to $\prod_{i=2}^{s} p_i^{k_i}$ so $\phi(n) = \phi(p_1^{k_1})\phi\left(\prod_{i=2}^{s} p_i^{k_i}\right) = p_1^{k_1-1}(p_1 - 1)\prod_{i=2}^{s} p_i^{k_i}$. Continue in the same way (more formally: use induction) to obtain the required formula. □

Example (calculation of $\phi(100)$)**.** $\phi(100) = 40$. Indeed, using Proposition 6.12, $100 = 2^2 5^2$, 2^2 is coprime to 5^2 hence $\phi(100) = \phi(2^2)\phi(5^2)$, $\phi(2^2) = 2^2 - 2^1 = 2$, $\phi(5^2) = 5^2 - 5^1 = 20$.

The following is a generalization of Fermat's Little Theorem to composite moduli.

Theorem 6.13 (Euler's Theorem)**.** If $\gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \mod n.$$

Proof. We start with the following

Claim. If $\gcd(a, n) = 1$, then the function $f \colon \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by the rule $f([x]_n) = [a]_n[x]_n$ is bijective.

Proof of the claim: $\gcd(a, n) = 1$ implies that the class $[a]_n \in \mathbb{Z}_n^*$ is invertible. Consider the function $g \colon \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $g([x]_n) = [a]_n^{-1}[x]_n$. Then $f(g([x]_n)) = g(f([x]_n)) = [x]_n$ for all $[x]_n \in \mathbb{Z}_n^*$, hence g is the inverse function to f. A function which has an inverse is a bijection. The claim is proved.

To prove Euler's Theorem, denote by X the product of all elements of $\mathbb{Z}_n^*$.

$$X = \prod_{[x]_n \in \mathbb{Z}_n^*} [x]_n.$$

If we apply f to each factor in this product, we will get the same factors but perhaps in a different order, because f is a bijection. Hence the product will not change:

$$X = \prod_{[x]_n \in \mathbb{Z}_n^*} f\left([x]_n\right)$$

Therefore, by definition of the function f,

$$X = \prod_{[x]_n \in \mathbb{Z}_n^*} ([a]_n[x]_n) = [a]_n^{|\mathbb{Z}_n^*|} \times \prod_{[x]_n \in \mathbb{Z}_n^*} [x]_n = [a]_n^{|\mathbb{Z}_n^*|}X.$$

Since $X \in \mathbb{Z}_n^*$, X has an inverse in $\mathbb{Z}_n^*$. Multiply through by X^{-1}:

$$[a]_n^{|\mathbb{Z}_n^*|} = [1]_n$$

which is equivalent to $a^{|\mathbb{Z}_n^*|} \equiv 1 \mod n$. Since $|\mathbb{Z}_n^*| = \phi(n)$ by definition of $\phi(n)$, Euler's Theorem is proved. □

Remark. Taking $n = p$, prime, in the Theorem we recover Fermat's Little Theorem. Indeed, $\phi(p) = p - 1$.

Example (calculation from chapter 3 revisited)**.** Given $\phi\left(100\right) = 40$ from above, find the last *two* digits in the decimal expansion of 1913^{99}.

Solution. We have to calculate the remainder of 1913^{99} when divided by 100 which is congruent to $13^{99} \mod 100$.

Euler's Theorem tells us that $13^{\phi(100)} = 13^{40} \equiv 1 \mod 100$. Thus

$$13^{99} = \left(13^{40}\right)^2 13^{19} \equiv 1^2 13^{19} \equiv 13^{19} \mod 100.$$

Now use a few steps of successive squaring:

		$\mod 100$
13^2		$\equiv 69$
13^4	$\equiv 69^2$	$\equiv 61$
13^8	$\equiv 61^2$	$\equiv 21$
13^{16}	$\equiv 21^2$	$\equiv 41$

Hence

$$\begin{aligned} 13^{99} \equiv 13^{19} &= 13^{16} \times 13^2 \times 13 \\ &\equiv 41 \times 69 \times 13 \\ &\equiv \qquad\qquad\qquad\qquad 77 \mod 100. \end{aligned}$$

So the last two digits of 13^{99} are 77, as already found earlier.

Remark (difficulty of finding $\phi(m)$)**.** You may now think that Euler's Theorem has none of the problems of Fermat's Little Theorem as we do not need to know that the modulus m is prime; Euler's Theorem holds for **all** m. But unfortunately it has another problem: how to calculate $\phi(m)$? The rules in proposition 6.12 allow you to calculate $\phi(m)$ for any m *provided* you can factor m. However, factorisation into primes is a very difficult problem for large m.

So much so that if one had a fast algorithm for calculating $\phi(m)$ one could break the ubiquitous **RSA public key encryption**. This has not happened yet.

Euler's and Fermat's Theorem: further examples

Not given in lectures. Students are advised to go through these examples in their own time.

Example. Find a solution to $x^{12} \equiv 3 \mod 11$.

Solution. Any solution of this must satisfy $\gcd(x, 11) = 1$ so Fermat's Little Theorem gives $x^{10} \equiv 1 \mod 11$. Thus our equation becomes

$$3 \equiv x^{12} \equiv x^2 x^{10} \equiv x^2 \mod 11.$$

Now check.

x	$x^2 \bmod 11$
1	1
2	4
3	9
4	5
5	3

Note that if $x \geq 6$ then $11 - x \leq 5$ and $x^2 \equiv (11-x)^2 \mod 11$ so all possible values of x^2 mod 11 will be seen in the table.

From the table we see **an** answer is $x \equiv 5 \mod 11$

Example. Show that $x^5 \equiv 3 \mod 11$ has **no** solutions.

Solution. By contradiction: assume $x^5 \equiv 3 \mod 11$ has solutions. Any solution of this must satisfy $\gcd(x, 11) = 1$ so Fermat's Little Theorem gives $x^{10} \equiv 1 \mod 11$. Since $5 \mid 10$ we square both sides of the original congruence to get

$$1 \equiv x^{10} \equiv \left(x^5\right)^2 \equiv 3^2 \equiv 9 \mod 11.$$

This is false and so the assumption is false and thus the congruence has no solution.

Example. Find *a* solution to $x^7 \equiv 3 \mod 11$.

Solution. Again $x^{10} \equiv 1 \mod 11$ by Fermat's Little Theorem but this time $7 \nmid 10$, in fact $\gcd(7, 10) = 1$. From Euclid's Algorithm we get

$$7 \times 3 - 10 \times 2 = 1$$

Raise both sides of the original congruence to the third power to get

$$\begin{aligned} 3^3 &\equiv \left(x^7\right)^3 \equiv x^{3\times 7} \equiv x^{1+2\times 10} \\ &\equiv x\left(x^{10}\right)^2 \equiv x \mod 11. \end{aligned}$$

Hence **a** solution is $x \equiv 3^3 \equiv 5 \mod 11$.

Don't forget to check your answer (by successive squaring of 5).

Example. Is $2^{35} + 1$ divisible by 11?

Solution. Here we look at $2^{35} + 1$ modulo 11. Because 11 is prime we could use Fermat's Little Theorem to say $2^{10} \equiv 1 \mod 11$. Thus

$$2^{35} + 1 \equiv 2^5 + 1 \equiv 32 + 1 = 33 \equiv 0 \mod 11,$$

i.e. $2^{35} + 1$ is divisible by 11.

Exercise. Show that $2^{1194} + 1$ is divisible by 65.

Interesting problems concerning primes

Not given in lectures. Interested students may find more information in the literature and online.

The following are conjectures and are all examples of problems that can be simply stated yet for which the answers are as yet unknown.

Goldbach's Conjecture. Is every even integer $n \geq 4$ the sum of two primes?

$$4 = 2 + 2, \qquad 6 = 3 + 3, \qquad 8 = 3 + 5, \qquad 10 = 3 + 7, \qquad 12 = 5 + 7,$$
$$14 = 3 + 11, \qquad 16 = 3 + 13, \qquad 18 = 5 + 13, \qquad 20 = 7 + 13, \ldots$$

Has been checked for all even numbers up to 4×10^{18} by Tomás Oliveira e Silva (as of 2017).

There is a proof (which is now being checked) that every even number $n \geq 4$ is the sum of *at most four* primes (Helfgott 2013).

Goldbach's Conjecture is a difficult problem because primes are *multiplicative* objects, defined in terms of divisibility, and yet this is an *additive* question.

Do there exist infinitely many Twin Primes, i.e. pairs of primes p and p' such that $p - p' = 2$? The first few examples are

$$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73),$$
$$(101,103), (107,109), (137,139), (149,151), (179,181), (191,193),$$
$$(197,199), (227,229), (239,241), \ldots .$$

A large prime pair is $2996863034895 \times 2^{1290000} \pm 1$, with 388,342 decimal digits. It was discovered in September 2016.

It has recently been proved (2014) that there are infinitely many pairs of primes $p < p'$ with $p' - p < 246$.

Is $n^2 + 1$ prime infinitely often?

$$2^2 + 1 = 5, \qquad 4^2 + 1 = 17, \qquad 6^2 + 1 = 37, \qquad 10^2 + 1 = 101, \qquad 14^2 + 1 = 197, \ldots$$

It has been shown that $n^2 + 1$ is either a prime or the product of two primes infinitely often.

For all $m \geq 1$ does there exists a prime p: $m^2 \leq p \leq (m+1)^2$?

What is known is **Theorem** (**Bertrand's postulate**): For all $N \geq 1$ there exists a prime $p : N \leq p \leq 2N$. (*Not proved in the course.*)

Definition (The Prime Counting Function). If $N \in \mathbb{N}$, we define

$$\pi(N) = |\{p : p \leq N,\ p \text{ is prime}\}| .$$