6 Prime Numbers

Part VI of PJE

6.1 Fundamental Results

Definition 6.1 *(p.277) A positive integer n is **prime** when $n > 1$ and the only positive divisors are 1 and n. Alternatively*

$$D(p) = \{-p, -1, 1, p\}.$$

*Otherwise $n > 1$ is said to be **composite**.*

So $n > 1$ is composite if, and only if, there exist integers $a > 1$ and $b > 1$ such that $n = ab$.

The integer $n = 1$ is neither prime nor composite.

Example 6.2 *The first few prime numbers are*

$$2, 3, 5, 7, 11, 13, 17, 19, ...$$

> **Aside** 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 $2^{57,885,161} - 1$ with $17,425,170$ digits, found on January 25^{th}, 2013, by the Great Internet Mersenne Prime Search **End of aside**

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

Lemma 6.3 *If p is prime and $p \nmid a$ then p and a are coprime.*

Proof Because p is prime its only divisors are $\pm p$ and ± 1, i.e.

$$D(p) = \{-p, -1, 1, p\}.$$

Since $p \nmid a$ the only *common* divisors of p and a are ± 1, i.e. $D(a, p) = \{-1, 1\}$. The greatest of these is 1, i.e. $\gcd(p, a) = 1$ which is the definition of coprime. ■

Theorem 6.4 *Every integer $n > 1$ is a product of primes.*
(With the convention that a product can be of just one prime!)

Proof See p.278. It is by *strong* induction, where to prove $P(n)$ for all n, you assume $P(j)$ holds for all $j \leq k$ and then use this assumption to prove that $P(k + 1)$ holds.

Theorem 6.5 *(Euclid) If $p|ab$ then either $p|a$ or $p|b$.*

Proof See p.279

> **Aside** This result motivates the definition of a prime in more advanced work. **End of aside**

Euclid's Theorem can be rewritten as saying that if p is prime and $p|m$ then, *for all* factorisations of $m = ab$ into integers, p must divide *at least one* of a or b.

Example 6.6 *Trivially* $6|24$*, yet* $24 = 3 \times 8$ *and* $6 \nmid 3$ *and* $6 \nmid 8$*. Hence* 6 *is not prime.*

Corollary 6.7 *If $p|a_1a_2...a_n$ then $p|a_i$ for some $1 \leq i \leq n$.*

Proof p.282 but here I give an alternative proof. Write our assumption $p|a_1a_2...a_n$ as $p|a_1\,(a_2...a_n)$ .Then Theorem 6.5, implies that either $p|a_1$ or $p|a_2...a_n$. If $p|a_1$ we are finished. If $p|a_2...a_n$ repeat the process. This 'algorithm' must end after at most $n-1$ steps. ■

Now we can prove that the product of primes guaranteed by Theorem 6.4 is unique (up to ordering).

Theorem 6.8 ***Fundamental Theorem of Arithmetic****. Every positive integer greater than 1 can be written as a product of primes unique up to ordering, i.e. for all $n \geq 2$*

$$n = p_1p_2...p_r$$

where each $p_i\,(i = 1, ..., r)$ is a prime.

Proof See p.283 for the proof by contradiction.

Aside It must be stressed that it is a very hard problem to find the prime decomposition of large numbers, harder than checking if a number is prime or not. What do I mean by large? A 232 digit was factored on December 12, 2009:

$$
\begin{aligned}
& 1230186684530117755130494958384962720772853569 \\
& 5953347921973224521517264005072636575187452021 \\
& 9978646938995647494277406384592519255732630345 \\
& 3731548268507917026122142913461670429214311602 \\
& 2212404792747377940806653514195974598569021434 13 \\
= \; & 3347807169895689878604416984821269081770479498 \\
& 3713768568912431388982883793878002287614711652 5 \\
& 3174308773781446799948 9 \\
\times \; & 3674604366679959042824463379962795263 22 \\
& 7915816434308764267603228381573966651 12 \\
& 7923337341714339681027009279873630891 7.
\end{aligned}
$$

See http://en.wikipedia.org/wiki/RSA_numbers. **End of aside**

Question How to find primes?

Aside In the Maths Workshop MATH10001 there was an exercise to use MATLAB to find the primes between 1 and 100. The idea could have been to identify the composites and discard them. You may have found a composite $a > 1$ by finding a factor $b > 1$ of a, i.e. $b|a$. So, for each a you would look at each $1 < b < a$ to see if $b|a$. In MATLAB you might use $\text{rem}(a, b) = 0$ iff b divides a. This is quite inefficient. To find a composite a it suffices to find a *prime* divisor of a. Thus you would look at the primes $1 < p < a$ to see if $p|a$. This is more efficient since there are fewer primes. But this can be made far more efficient by the next result. If we are looking for primes $\leq N$ we need only examine each $a \leq N$ and look to see if there are any primes $p \leq \sqrt{N}$ which divide a, i.e. $p|a$. That is, instead of looking at primes $p < a$ we need only look at $p < \sqrt{N}$. If a is close to N this is a substantial saving. **End of aside.**

Theorem 6.9 *If m is composite then m has a prime divisor not exceeding $\sqrt{m}$. That is,*

$$\forall \text{ composite } m > 1, \exists p : p|m \text{ and } p \leq \sqrt{m}.$$

Proof The proof found on page p.280 is direct. Here we give an alternative proof by contradiction.

Assume for contradiction the negation of what you want to prove. In symbols,

$$\exists \text{ composite } m > 1, \forall p, p|m \Rightarrow p > \sqrt{m}, \tag{1}$$

whilst in words, there exists a composite integer m whose prime divisors are are strictly greater than $\sqrt{m}$.

(We have seen before that the negation of '$p \Rightarrow q$' is 'p and not q', and so the negation of 's and r' is '$s \Rightarrow$ not r'. This is applied here with $s \equiv p|m$ and $r \equiv p \leq \sqrt{m}$.)

Since m is composite it can be factored as $m = ab$ with $1 < a, b < m$.

From $a > 1$ we have, by Theorem 6.4, that a is a product of primes. If p is one of the primes in the product than $p|a$, which implies $p \leq a$.

Similarly, because $b > 1$ we can again find a prime q which divides b, which implies $q \leq b$.

Thus $pq \leq ab = m$.

But $p|a$ and $a|m$ combine to give $p|m$ in which case $p > \sqrt{m}$, by (1) .
Similarly, $q|b$ and $b|m$ implies $q|m$ in which case $q > \sqrt{m}$, again by (1) .
Hence $pq > (\sqrt{m})^2 = m$.

Therefore we have both $pq \leq m$ and $pq > m$, a contradiction.

Thus our assumption is false, and so all composite numbers $m > 1$ have at least one prime divisor $\leq \sqrt{m}$. ■

Application *Sieve of Eratosthenes*,

- Write out the list of natural numbers from 2 up to N.
- Strike out all multiples of 2, except for 2.
- 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 $> \sqrt{N}$.

Since we are striking out multiples we are **only** striking out composite numbers. Since every composite number $m \leq N$ has, by the previous result, a (prime) divisor $\leq \sqrt{m} \leq \sqrt{N}$, we will strike out **every** composite number $\leq N$. Thus what will remain will be the non-composite numbers, i.e. the primes, between 2 and N.

So, for example, if we look for primes up to 100 we need only check for divisibility by primes up to $\sqrt{100} = 10$, i.e. 2, 3, 5 and 7. *See Appendix 7-i where this is carried out for* $N = 100$.

Question How many primes are there?

Theorem 6.10 *There are infinitely many primes.*

Proof (due to Euler) p.285 is by assuming there are only finitely many primes, labelled $p_1, ..., p_r$ and looking at $N = p_1 p_2 ... p_r + 1$. ■

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

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

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

6.2 Interesting problems concerning primes.

Not given in lectures.

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

1) ***Goldbach's Conjecture***, Is every even integer $n \geq 4$ the sum of two primes?

$$\begin{aligned} 4 &= 2+2, \quad 6=3+3, \quad 8=3+5, \quad 10=3+7, \quad 12=5+7, \\ 14 &= 3+11, \quad 16=3+13, \quad 18=5+13, \quad 20=7+13, ... \end{aligned}$$

Has been checked for all even numbers up to 12×10^7 by Oliveira e Silva (July 14, 2008).

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

2) ***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

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

A large prime pair is $65516468355 \times 2^{333333} \pm 1$ with 100355 digits discovered by Kaiser1 & Klahn in 2009.

It has recently been proved (2014) that there are infinitely many pairs of primes $p < p'$ (not necessarily consecutive) with $p' - p < 246$.

3) ***Is*** n^2+1 ***prime infinitely often***?

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

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

4) ***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 $p : N \leq p \leq 2N$.

Proof not given in course.

6.3 Fermat's Little Theorem

Theorem 6.11 *If p is prime then p divides $\binom{p}{r}$, i.e.*

$$p \left| \binom{p}{r} \right. ,$$

for $1 \leq r \leq p-1$.

Proof Recall that the Binomial Number can be written in a form involving factorials.

$$\binom{p}{r} = \frac{p!}{r!\,(p-r)!}.$$

Multiply up as

$$p! = r!\,(p-r)!\binom{p}{r}. \tag{2}$$

Since $p! = p\,(p-1)!$ we see that $p|p!$. Thus $p|\text{LHS}\,(2)$ and so $p|\text{RHS}\,(2)$, i.e.

$$p|r!\,(p-r)!\binom{p}{r}.$$

Yet p is prime so by the corollary to Euclid's Theorem above p must divide at least one of

$$r!, \quad (p-r)! \quad \text{or} \quad \binom{p}{r}.$$

If $p|r! = r\,(r-1)\,....2.1$ then again by the corollary to Euclid's Theorem we have that p divides one of the factors, i.e. $p|j$ for some $1 \leq j \leq r$. Yet $p|j$ implies $p \leq j$ while we are told, in the assumptions of the Theorem, that $r \leq p-1$. Combined together we get $p \leq j \leq r \leq p-1$, i.e. $p \leq p-1$, impossible.

Similarly, if $p|\,(p-r)!$ then $p|j$ for some $1 \leq j \leq p-r$. Then $p \leq j \leq p-r \leq p-1$, since $r \geq 1$. Again impossible.

As Sherlock Holmes said, "when you have eliminated the impossible, whatever remains, however improbable, must be the truth". Hence

$$p \left| \binom{p}{r} \right. .$$

■

On Problem Sheet 1 you were asked to show that $n^5 \equiv n \bmod 5$ for all $n \geq 1$. The hint was to use induction and the Binomial Theorem on $(k+1)^5$ which gives

$$(k+1)^5 = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 \equiv k + 1 \bmod 5. \tag{3}$$

The following result generalises this.

Theorem 6.12 *For all $a, b \in \mathbb{Z}$ and all primes p we have*

$$(a+b)^p \equiv a^p + b^p \bmod p. \tag{4}$$

Proof in lectures. Follows immediately from the Binomial Theorem and previous result. ■

Then, just as (3) can be used to prove $n^5 \equiv n \bmod 5$ for all $n \geq 1$, (4) can be used to prove the following general result.

Corollary 6.13 *(**Fermat's Little Theorem**) For all $n \geq 1$, and all primes p,*

$$n^p \equiv n \bmod p.$$

If $\gcd(p, n) = 1$ *then*

$$n^{p-1} \equiv 1 \bmod p.$$

Proof in lectures. By induction based on $(n+1)^p \equiv n^p + 1 \bmod p$ which follows from (4). ■

6.4 Application: finding and using inverses.

Fermat's Little Theorem has numerous applications, including simplifying the calculation of powers in modular arithmetic. From the theorem we see that if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$, or equivalently $a^{p-2} \times a \equiv 1 \bmod p$. This means that a^{p-2} is the inverse of a modulo p or, in the language of congruence classes,

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

Aside An interesting question is with which method is it *quickest* to calculate the modular inverse an integer modulo a 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 a. For Euclid's algorithm this result on the running time is the content of Lame's Theorem, PJE p.226. **End of aside**

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

Example 6.14 *Find the integer solutions of* $5x \equiv 6 \bmod 19$.

Solution 19 is prime so Fermat's Little theorem implies $5^{18} \equiv 1 \bmod 19$. So $5 \times 5^{17} \equiv 1 \bmod 19$, i.e. 5^{17} is the inverse of $5 \bmod 19$. Thus multiplying both sides of the equation by 5^{17} gives

$$5^{18}x \equiv 6 \times 5^{17} \bmod 19, \text{ i.e. } x \equiv 6 \times 5^{17} \bmod 19.$$

Though this is **an** answer to the question we normally give x as the *least positive residue*. Successive squaring gives

$$5^2 \equiv 6, 5^4 \equiv 17, 5^8 \equiv 4 \text{ and } 5^{16} \equiv 16 \bmod 19.$$

Thus

$$x \equiv 6 \times 5 \times 5^{16} \equiv 6 \times 5 \times 16 \equiv 5 \bmod 19,$$

which agrees with the answer found in Chapter 3, but which *should still be checked by substitution.* ■

6.5 Application: Calculating powers

With $p = 13$ and $a = 4$ we see that $4^{12} \equiv 1 \bmod 13$. Thus

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

as we have seen before in Chapter 3, using the method of successive squaring.

Aside 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. As already stressed, it is a difficult problem showing that a large number is prime. The largest known prime (as of September 2008) is $2^{43,112,609} - 1$. (See http://primes.utm.edu/largest.html for further details). **End of aside.**

6.6 Bijections from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$; 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

$$\{[r]_n : 1 \leq r \leq n, \gcd(r,n) = 1\},$$

which, because we can take different labels for the classes, is the same as

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

Definition 6.15 ***Euler's phi-function*** *is, for all $n \geq 1$, given by*

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

Examples

- 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 integers strictly less than p are coprime to p.
- 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 $\phi(10) = 4$.

Theorem 6.16 *a) If* $\gcd(m,n) = 1$ *then*

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

b) If p is prime then

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

for all $r \geq 1$.

Proof not given in this course, though **you** should be able to prove part b . ■

Example $\phi(100) = 40$.

Solution See appendix for a counting argument. Starting from the Theorem we have

$$\begin{aligned}\phi(100) &= \phi\left(5^2 \times 4\right) = \phi\left(5^2\right)\phi(4) \\ &= 5 \times (5-1) \times 2 = 40.\end{aligned}$$

■

Theorem 6.17 *If* $\gcd(a,n) = 1$ *then the function*

$$\rho_a : \mathbb{Z}_n^* \to \mathbb{Z}_n^*, [r]_n \mapsto [ar]_n$$

is a bijection.

Proof The idea for the proof can be seen on p.259 and p.290.

Is the function well-defined, i.e. does the image lie in $\mathbb{Z}_n^*$? Assume $[r]_n \in \mathbb{Z}_n^*$ so $\gcd(r,n) = 1$ by definition of $\mathbb{Z}_n^*$. By the assumption in the theorem we have $\gcd(a,n) = 1$. Combine to get $\gcd(ar,n) = 1$ in which case $[ar]_n \in \mathbb{Z}_n^*$. Hence for every $[r]_n \in \mathbb{Z}_n^*$ the image $\rho_a([r]_n)$ is in $\mathbb{Z}_n^*$ and so the function is well-defined.

Is the function a bijection? Recall that a function $f : A \to A$ where A is a finite set is a bijection if, and only if, it is an injection. Thus to show that ρ_a is a bijection it suffices to show that ρ_a is an injection.

To show that ρ_a is injective (i.e. 1-1) assume $\rho_a([r_1]_n) = \rho_a([r_2]_n)$. Then

$$\begin{aligned}\rho_a([r_1]_n) = \rho_a([r_2]_n) &\Rightarrow [ar_1]_n = [ar_2]_n, \quad \text{by definition of } \rho_a, \\ &\Rightarrow ar_1 \equiv ar_2 \bmod n, \\ &\Rightarrow r_1 \equiv r_2 \bmod n, \quad \text{since } \gcd(a,n) = 1, \\ &\Rightarrow [r_1]_n = [r_2]_n.\end{aligned}$$

Thus ρ_a is injective, and therefore a bijection on $\mathbb{Z}_n^*$. ■

Example On $\mathbb{Z}_8^* = \{1,3,5,7\}$, consider ρ_3.

$$\begin{aligned}\rho_3([1]_8) &= [3]_8, \\ \rho_3([3]_8) &= [9]_8 = [1]_8, \\ \rho_3([5]_3) &= [15]_8 = [7]_8, \\ \rho_3([7]_8) &= [21]_8 = [5]_8.\end{aligned}$$

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

Theorem 6.18 ***Euler's Theorem*** *If* $\gcd(a,n)=1$ *then*

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

Proof is **not** in PJE's book, but the idea is to be found on p.290.

Since ρ_a is a bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_n^*$ then the image of ρ_a is simply $\mathbb{Z}_n^*$ in *some different order.* Since order is immaterial in sets we have $\mathbb{Z}_n^* = \operatorname{Im}\rho_a$, i.e.

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

Taking products of everything in each set we get

$$\prod_{\substack{1\le r\le n\\ \gcd(r,n)=1}} [r]_n = \prod_{\substack{1\le r\le n\\ \gcd(r,n)=1}} [ar]_n = \prod_{\substack{1\le r\le n\\ \gcd(r,n)=1}} ([a]_n [r]_n)$$

by definition of multiplication in $\mathbb{Z}_n$

$$= [a]_n^{\phi(n)} \prod_{\substack{1\le r\le n\\ \gcd(r,n)=1}} [r]_n,$$

since there are $\phi(n)$ terms in the product. Now cancel the product from both sides to get

$$[1]_n = [a]_n^{\phi(n)} = \left[a^{\phi(n)}\right]_n,$$

again by the definition of the multiplication of classes. But this final result merely means $a^{\phi(n)} \equiv 1 \bmod n$, as required. ■

Example of *the method of proof* of Euler's Theorem.

Not given.

$\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$, and so $\phi(8) = 4$ (though this was seen earlier)..

Take $a = 5$, in which case the map ρ_5 is

$$\begin{aligned} [1]_8 &\mapsto [5\times 1]_8 = [5]_8, \\ [3]_8 &\mapsto [5\times 3]_8 = [7]_8, \\ [5]_8 &\mapsto [5\times 5]_8 = [1]_8, \\ [7]_8 &\mapsto [5\times 7]_8 = [3]_8. \end{aligned}$$

Then

$$\begin{aligned}[1]_8\,[3]_8\,[5]_8\,[7]_8 &= [5\times 1]_8\,[5\times 3]_8\,[5\times 5]_8\,[5\times 7]_8\\ &= [5]_8^4\,[1]_8\,[3]_8\,[5]_8\,[7]_8\end{aligned}$$

Cancelling the product $[1]_8\,[3]_8\,[5]_8\,[7]_8$ from both sides leaves $[5]_8^4 = [1]_8$. Thus

$$5^4 \equiv 1 \bmod 8$$

as expected. ■

Taking $n = p$, prime, in the Theorem we recover

Theorem 6.19 ***Fermat's Little Theorem*** *If p is prime and a an integer with $p \nmid a$ then*

$$a^{p-1} \equiv 1 \bmod p. \tag{5}$$

Proof See p.290.

Corollary 6.20 *If p is prime and a an integer then $a^p \equiv a \bmod p$.*

Proof Either $p \nmid a$ or $p|a$.

If $p \nmid a$ then Fermat's Little Theorem implies $a^{p-1} \equiv 1 \bmod p$. Multiply by a to get $a^p \equiv a \bmod p$.

If $p|a$ then $a \equiv 0 \bmod p$. But then $a^{p-1} \equiv 0 \bmod p$ and so $a^{p-1} \equiv 0 \equiv a \bmod p$.

In both cases we have $a^p \equiv a \bmod p$. ■

Note that this version of Fermat's Last Theorem holds for both positive and negative a whereas the earlier version, proved by induction, held only for positive a.

Example 6.21 *Given $\phi(100) = 40$ from above, find the last two digits in the decimal expansion of 13^{99}.*

Solution We have to calculate $13^{99} \bmod 100$.

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

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

Now use successive squaring

$$\begin{aligned} 13^2 &\equiv 69, \\ 13^4 &\equiv 61, \\ 13^8 &\equiv 21, \\ 13^{16} &\equiv 41 \bmod 100. \end{aligned} \tag{6}$$

Hence

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

So the last two digits of 13^{99} are 77, as already found in Chapter 3. ■

> **Aside** 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** integers m. But unfortunately it has another problem, how to calculate $\phi(m)$? In general this is very difficult for large m. Together, $\phi(st) = \phi(s)\phi(t)$ if $\gcd(s,t) = 1$ and $\phi(p^r) = p^{r-1}(p-1)$ if p is prime, allow you to calculate $\phi(m)$ for any m *provided* you can factor m. Unfortunately, as noted previously, this is a very difficult problem for large m.

6.7 Applications of Euler's and Fermat's Theorem.

Not given

Example 6.22 *Find a solution to* $x^{12} \equiv 3 \bmod 11$.

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

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

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 $x^2 \equiv (11-x)^2 \bmod 11$ so all possible values of $x^2 \bmod 11$ will be seen in the table.

From the table we see **an** answer is $x \equiv 5 \bmod 11$. ■

Example 6.23 *Show that* $x^5 \equiv 3 \bmod 11$ *has* ***no*** *solutions.*

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

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

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

Example 6.24 *Find a solution to* $x^7 \equiv 3 \bmod 11$.

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

$$3 \times 7 - 2 \times 10 = 1. \tag{7}$$

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

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

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

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

iv) Is $2^{35} + 1$ divisible by 11? Here we look at $2^{35} + 1 \bmod 11$. Because 11 is prime we could use Fermat's Little Theorem to say $2^{10} \equiv 1 \bmod 11$. Thus

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

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

Question for students. Show that $2^{1194} + 1$ is divisible by 65.

7 Permutations

Very little of this section comes from PJE.

7.1 Definitions

Definition 7.1 *A **permutation** (p.147) of a set A is a bijection $\rho : A \to A$.*

Notation If $A = \{a, b, c, ...\}$ and ρ is a permutation on A we can express the action of ρ on A using a two row notation due to Cauchy:

$$\rho = \begin{pmatrix} a & b & c & \dots \\ \rho(a) & \rho(b) & \rho(c) & \dots \end{pmatrix}.$$

Note The ***identity map***, 1_A, which satisfies $1_A(\alpha) = \alpha$ for all $\alpha \in A$, is therefore given by

$$1_A = \begin{pmatrix} a & b & c & \dots \\ a & b & c & \dots \end{pmatrix}.$$

Definition 7.2

- *The collection of all permutations on a set A, denoted by S_A, is called the **symmetric group** on A.*
- *When $A = \{1, 2, 3, ..., n\}$, S_A is usually denoted by S_n, and is called the **symmetric group on** n **letters**.*
- *Let 1_n denote the identity map in S_n.*

  Aside One of the goals of this part of the course is to understand the words 'symmetric' and 'group'.

Example 7.3 *S_3 consists of*

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Recall a result from earlier in the course.

Theorem 7.4 *If A is a finite set then $f : A \to A$ is a bijection if, and only if, it is an injection.*

Proof p.138 but covered in the first half of the course.

Corollary 7.5 *If $|A| = n \geq 1$ then the number of permutations $\rho : A \to A$ is $n!$.*

Proof Since A is a finite set, to count bijections it suffices to count injections. Hence

$$|S_A| = |Inj\,(A, A)| = n!$$

■

In particular, $|S_3| = 3! = 6$. Since we found 6 different permutations above in S_3 we, in fact, found all the permutations in S_3.

7.2 Compositions

Recall, if ρ and π are functions $A \to A$, then the composite function is defined by

$$\rho \circ \pi\,(a) = \rho\,(\pi\,(a))$$

for all $a \in A$. Further, if ρ and π are bijections then $\rho \circ \pi$ is a bijection. Hence the composition of permutations is a permutation.

Example 7.6 *Let $\rho, \pi \in S_5$ be given by*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \quad \textit{and} \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Calculate $\rho \circ \pi$.

Solution To write $\rho \circ \pi$ in the same way we have to see first what π does to a given element of A and then secondly what ρ does to this image. In this example,

$$\begin{aligned}
\pi\,(1) &= 2, \quad \rho\,(2) = 2 \quad \text{so} \quad \rho \circ \pi\,(1) = 2, \\
\pi\,(2) &= 3, \quad \rho\,(3) = 1 \quad \text{so} \quad \rho \circ \pi\,(2) = 1, \\
\pi\,(3) &= 4, \quad \rho\,(4) = 3 \quad \text{so} \quad \rho \circ \pi\,(3) = 3, \\
\pi\,(4) &= 5, \quad \rho\,(5) = 5 \quad \text{so} \quad \rho \circ \pi\,(4) = 5, \\
\pi\,(5) &= 1, \quad \rho\,(1) = 4 \quad \text{so} \quad \rho \circ \pi\,(5) = 4.
\end{aligned}$$

Thus

$$\begin{aligned}\rho\circ\pi &= \begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}.\end{aligned}$$

■

Note we first looked at π then at ρ, so read $\rho\circ\pi$ ***from the right***.
Note also that

$$\pi\circ\rho = \begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix},$$

so that, for instance, $\rho\circ\pi(1)=2$ but $\pi\circ\rho(1)=5$. Thus

$$\rho\circ\pi\neq\pi\circ\rho,$$

and hence, composition of permutations is **not** commutative.

Inverses Recall, *a bijection always has an inverse.* The inverse of a permutation written in the two row manner can easily be found by exchanging upper and lower rows, and then reordering the columns so the entries on the upper row appear in the same order as in the original permutation.

Example 7.7 *In S_5 find the inverse of*

$$\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}$$

Solution

$$\begin{pmatrix}4&2&1&3&5\\1&2&3&4&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&2&4&1&5\end{pmatrix}.$$

■

You should check that your answer satisfies the definition of inverse, namely that $f\circ f^{-1}=f^{-1}\circ f=1$. Thus

$$\begin{aligned}&\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\3&2&4&1&5\end{pmatrix}\\ =&\begin{pmatrix}1&2&3&4&5\\3&2&4&1&5\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}=1_5\end{aligned}$$