Part A Number Theory 2009

Henri Johnston (henri@maths.ox.ac.uk)

21st May 2009

Note

These lecture notes are based on hand written notes by Dr. Tim Browning, who gave this course in 2004 and 2005. These notes were originally typeset by Andrew Caldwell who attended the lectures in 2007 and were subsequently amended by Professor Roger Heath-Brown. They have since been further checked and amended by me. While I take full responsibility for the present version (corrections and comments welcome), considerable thanks are clearly due to Tim Browning, Andrew Caldwell, and Roger Heath-Brown.

These notes are intended to complement rather than replace lectures (for instance, the diligent student should read at least one or two lectures ahead). Indeed, there may well be differences between these notes and what I write in lectures. Finally, I would encourage all students to consult the recommended texts, as they contain many more details and examples, and had much more time and effort put in to them, than these notes.

1 The Integers

We begin with a quick run through of material that has previously been covered in other courses.

Definition. In this course, $\mathbb{N} := \{1, 2, 3, \ldots\}$ (i.e. zero is not included).

Remark. $(\mathbb{Z}, +, \times)$ is a commutative ring with 1.

Definition. Given $a, b \in \mathbb{Z}$ with $b \neq 0$, we say that b divides a (and we write $b|a$) if and only if there exists $c \in \mathbb{Z}$ such that $a = bc$.

Theorem 1.1 (The Division Algorithm)**.** *Given $a \in \mathbb{Z}$, $b \in \mathbb{N}$, there exist unique integers q and r satisfying $a = bq + r$ and $0 \leq r < b$.*

Proof. Mods. □

Definition. Let $a, b \in \mathbb{Z}$, not both zero. The highest common factor of a and b, written (a, b), is defined to be the largest $n \in \mathbb{N}$ such that $n|a$ and $n|b$. If $(a, b) = 1$ then a and b are said to be coprime.

Remark. Note that this is *not* the definition of highest common factor used in rings in general, but can be shown to be equivalent to the general definition in the case of the ring $\mathbb{Z}$.

Theorem 1.2 (Euclid's Algorithm)**.** *Let $r_0 = a$, $r_1 = b$ be positive integers with $a \geq b > 0$ and apply the division algorithm successively to get $r_j = r_{j+1}q_{j+1} + r_{j+2}$ with $0 < r_{j+2} < r_{j+1}$ for $0 \leq j \leq n-2$ and $r_{n+1} = 0$. Then the last non-zero remainder r_n is equal to (a, b).*

Proof. Mods. □

Lemma 1.3. *Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $u, v \in \mathbb{Z}$ such that $au + bv = (a, b)$.*

Proof. Mods — Work backwards through Euclid's algorithm. □

Example. Work out the highest common factor of 841 and 160 and express it as a linear combination of 841 and 160:

$$\begin{aligned} 841 &= 160 \times 5 + 41 \\ 160 &= 41 \times 3 + 37 \\ 41 &= 37 \times 1 + 4 \\ 37 &= 4 \times 9 + 1 \\ 4 &= 1 \times 4 + 0. \end{aligned}$$

Hence $(841, 160) = 1$ (i.e. they are coprime) and working backwards gives:

$$\begin{aligned} 1 &= 37 \times 1 - 4 \times 9 \\ &= 37 \times 1 - (41 - 37) \times 9 \\ &= 37 \times 10 - 41 \times 9 \\ &= (160 - 3 \times 41) \times 10 - 41 \times 9 \\ &= 160 \times 10 - 41 \times 39 \\ &= 160 \times 10 - (841 - 160 \times 5) \times 39 \\ &= -39 \times 841 + 205 \times 160. \end{aligned}$$

Note that such a solution is not unique. For example, we will also have

$$1 = (160 - 39) \times 841 + (205 - 841) \times 160 = 121 \times 841 - 636 \times 160.$$

Lemma 1.4. *Let $h = (a, b)$. Then $m|a$ and $m|b$ if and only if $m|h$.*

Proof. ($\Leftarrow$) Suppose $m|h$. By definition of h, $h|a$. Hence $m|a$. Similarly, $m|b$.

($\Rightarrow$) Assuming $m|a$ and $m|b$, we see that $a = ma'$ and $b = mb'$, say. Now, by Lemma 1.3, there exist $u, v \in \mathbb{Z}$ such that $au + bv = h$ and hence $h = m(a'u + b'v)$. Therefore $m|h$. □

Lemma 1.5. *Let $a, b \in \mathbb{Z}$, not both zero.*

(i) If $(a, b) = d$ *then* $(\frac{a}{d}, \frac{b}{d}) = 1$.

(ii) If $c \in \mathbb{Z}$ *then* $(a + cb, b) = (a, b)$.

Proof. (i) Suppose $e \in \mathbb{N}$ such that $e|\frac{a}{d}$ and $e|\frac{b}{d}$. Then there exist $m, n \in \mathbb{Z}$ with $\frac{a}{d} = em$, $\frac{b}{d} = en$. Hence $a = edm$ and $b = edn$, so that ed divides a and b. However, d is the largest such integer, whence $ed \leq d$. Thus we can only have $e = 1$.

(ii) Suppose $(a + bc, b) = e$. Then $e|(a + bc)$ and $e|b$. However, $e|b \Rightarrow e|bc$ and $e|(a + bc)$, $e|bc \Rightarrow e|a$. Thus $e|a$ and $e|b$ and hence $(a, b) \geq e$. Conversely, if $(a, b) = f$, then $f|a$ and $f|b$, whence $f|bc$. It follows that $f|(a + bc)$, and since $f|b$ we must have $f \leq (a + bc, b) = e$. Hence both $f \geq e$ and $e \geq f$, so that $e = f$.

□

Lemma 1.6. *Let* $a, b, c \in \mathbb{Z}$ *with* a, b *both non-zero.*

(i) The equation $ax + by = c$ *is soluble with* $x, y \in \mathbb{Z}$*, if and only if* $(a, b)|c$.

(ii) If $(a, c) = 1$*, then* $c|ab$ *if and only if* $c|b$.

Proof. (i) ($\Rightarrow$) By Lemma 1.4, $(a, b)|a$ and $(a, b)|b$, so that if $c = ax + by$ then c is also a multiple of (a, b). ($\Leftarrow$) Suppose $(a, b)|c$ and write $c = (a, b)q$. Then there exist $x, y \in \mathbb{Z}$ such that $(a, b) = ax + by$, by Lemma 1.3. Hence $c = q(a, b) = qxa + qyb$, which gives a suitable solution.

(ii) $c|b \Rightarrow c|ab$ is obvious. Suppose that $(a, c) = 1$ and $c|ab$. Then by Lemma 1.3, there exist $x, y \in \mathbb{Z}$ such that $1 = ax + cy$, whence $b = b \times 1 = abx + cby$. Now $c|ab$ and $c|cb$, so $c|b$.

□

Definition. Prime and composite numbers in $\mathbb{N}$:

(i) A number $p \in \mathbb{N}$ with $p \geq 2$ is prime if and only if its only divisors are 1 and p.

(ii) A number $n \in \mathbb{N}$ with $n \geq 2$ is composite if and only if it is not prime.

Note that $n = 1$ is neither prime nor composite.

Remark. Suppose p is prime and $p|ab$. Let $h = (p, a)$. Then $h|p$ so that $h = 1$ or $h = p$. If $h = 1$ then, by Lemma 1.6, $p|b$. If $h = p$ then $p = h|a$ (since $h = (a, b)$). Hence $p|a$ or $p|b$. For rings in general, the property that $p|ab \Rightarrow p|a$ or $p|b$ is taken as the defining property for primes.

Theorem 1.7 (The Fundamental Theorem of Arithmetic)**.** *Each* $n \in \mathbb{N}$ *can be expressed as a product of prime power factors in exactly one way, up to the ordering of the factors.*

Proof. Given in the Part A Algebra course. However, here is a sketch.

Existence of factorisations can be shown by induction on n. The case $n = 1$ is the empty product of primes. In general, if $1, \ldots, (n-1)$ are products of primes, then either n is prime or $n = ab$ with $1 < a, b < n$ and a, b are products of primes.

To show uniqueness, suppose that $n = p_1 \ldots p_r = q_1 \ldots q_s$ where the p_i's are q_j's are prime. Then $p_1 | (q_1 \ldots q_s)$, so Lemma 1.6 (with an induction argument) shows that $p_1 | q_j$ for some j. Since q_j is prime, we must have $p_1 = q_j$. Now cancel a factor and repeat the argument. □

Remark. Given $a, b \in \mathbb{N}$, we may write

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

where the p_i's are distinct primes and $\alpha_i, \beta_j \in \mathbb{N} \cup \{0\}$. Then

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n},$$

where $\gamma_i = \min(\alpha_i, \beta_i)$.

Theorem 1.8 (Euclid)**.** *There are infinitely many primes.*

Proof. For a contradiction, assume $\{p_1, p_2, \ldots, p_n\}$ is a complete list of primes. Consider $N := 1 + p_1 p_2 \ldots p_n \in \mathbb{N}$. Then $N \geq 2$ and so either N is prime or it has a prime factor. Thus there exists a prime p dividing N. However, every prime is supposedly one of $p_1, \ldots, p_n$, whence $p = p_i$ for some i. Then $p = p_i | (p_1 \ldots p_n)$, whence $p | (N-1)$. However we also have $p | N$, so $p | 1$. ※ □

2 Linear Congruences

Definition. Suppose that $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $a \equiv b \mod n$ (or $a \equiv b \pmod{n}$), and say a is congruent to b mod n, if and only if $n | (a - b)$.

Example. $4 \equiv 30 \mod 13$ since $13 | (4 - 30) = -26$

Lemma 2.1. *Let $n \in \mathbb{N}$. Then:*

(i) being congruent mod n is an equivalence relation.

(ii) if $a \equiv \alpha \mod n$ and $b \equiv \beta \mod n$ then $a+b \equiv \alpha+\beta \mod n$, $a-b \equiv \alpha-\beta \mod n$ and $ab \equiv \alpha\beta \mod n$. Moreover, if $f(x) \in \mathbb{Z}[x]$ then $f(a) \equiv f(\alpha) \mod n$.

Proof. (i) Exercise.

(ii) We will check that $ab \equiv \alpha\beta \mod n$; the rest is an exercise. Since $a \equiv \alpha \mod n$, we have $n | (a - \alpha)$ and so $a = \alpha + ns$ for some $s \in \mathbb{Z}$. Similarly, $b = \beta + nt$ for some $t \in \mathbb{Z}$. Hence $ab = (\alpha + ns)(\beta + nt) = \alpha\beta + n(s\beta + t\alpha + nst)$ and so $n | (ab - \alpha\beta)$. Therefore $ab \equiv \alpha\beta \mod n$, as required.

□

Example. Let $n \in \mathbb{N}$ and write n in decimal notation

$$n = \sum_{i=0}^{k} a_i \times 10^i \text{ where } 0 \leq a_i \leq 9 \text{ and } a_i \in \mathbb{N} \text{ for all } i.$$

Define $f(x)$ by

$$f(x) = \sum_{i=0}^{k} a_i x^i.$$

Then, since $10 \equiv -1 \mod 11$, we see that $n = f(10) \equiv f(-1) \mod 11$, whence $11|n \iff 11|f(-1) \iff 11|(a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^k a_k)$. This gives an easy way to test integers for divisibility by 11.

Definition. Given $n \in \mathbb{N}$, we write $[a]_n$ for the equivalence class of a, so that $[a]_n = \{b \in \mathbb{Z} : a \equiv b \mod n\}$.

Remark. We have $\mathbb{Z} = \bigcup_{a=0}^{n-1} [a]_n$ (disjoint equivalence classes).

Definition. We write $\mathbb{Z}/n\mathbb{Z} = \{[a]_n : 0 \leq a \leq n-1\}$ (so that $\#(\mathbb{Z}/n\mathbb{Z}) = n$). We set $[a]_n + [b]_n := [a+b]_n$ and $[a]_n[b]_n := [ab]_n$ (we must check that these are well-defined).

Lemma 2.2. *The set $\mathbb{Z}/n\mathbb{Z}$, with the above operations, is a commutative ring with $0 = [0]_n$ and $1 = [1]_n$.*

Proof. Given in Part A Algebra. □

Definition. We write

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \exists [b]_n \in \mathbb{Z}/n\mathbb{Z} \text{ such that } [a]_n[b]_n = [1]_n\}.$$

This is the set of units of $\mathbb{Z}/n\mathbb{Z}$, and is a group under multiplication.

Lemma 2.3. $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \iff (a, n) = 1$.

Proof.

$$\begin{aligned}
[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times &\iff \exists [b]_n \in (\mathbb{Z}/n\mathbb{Z}) \text{ such that } [a]_n[b]_n = [1]_n \\
&\iff \exists b \in \mathbb{Z} \text{ such that } [ab]_n = [1]_n \\
&\iff \exists b \in \mathbb{Z} \text{ such that } ab \equiv 1 \mod n \\
&\iff \exists b \in \mathbb{Z} \text{ such that } n|(ab-1) \\
&\iff \exists b, t \in \mathbb{Z} \text{ such that } ab - 1 = nt \\
&\iff (a, n) = 1, \text{ by Lemma 1.6.}
\end{aligned}$$

□

Example. $\left(\frac{\mathbb{Z}}{12\mathbb{Z}}\right)^\times = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

Lemma 2.4. *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$.*

(i) The congruence $ax \equiv b \mod n$ has a solution $x \in \mathbb{Z}$ if and only if $(a,n)|b$.

(ii) If $(a,n)|b$ then $\#\{[x]_n : ax \equiv b \mod n\} = (a,n)$.

Proof. (i) There exists $x \in \mathbb{Z}$ such that $ax \equiv b \mod n$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax - b = ny$ if and only if $(a,n)|b$, by Lemma 1.6.

(ii) Let $(a,n) = h$ with $h|b$. By part (i), $ax_0 - b = ny_0$ for some x_0, y_0. Then

$$\begin{aligned} ax - b = ny &\iff ax - ny = b = ax_0 - ny_0 \\ &\iff a(x - x_0) = n(y - y_0) \\ &\iff \frac{a}{h}(x - x_0) = \frac{n}{h}(y - y_0). \end{aligned}$$

But $\left(\frac{a}{h}, \frac{n}{h}\right) = 1$ by Lemma 1.5, whence $\frac{a}{h}|(y - y_0)$ and $\frac{n}{h}|(x - x_0)$. Then if $y - y_0 = \frac{a}{h}t$ say, we have $x - x_0 = \frac{n}{h}t$, so that

$$\{x : ax \equiv b \mod n\} = \{x = x_0 + \frac{n}{h}t : t \in \mathbb{Z}\}.$$

Thus we get distinct classes $[x]_n$ for $0 \leq t < h$, and hence

$$\#\{[x]_n : ax \equiv b \mod n\} = h = (n,a).$$

□

Example. Find the solutions of $100x \equiv 26 \mod 86$. We have $100x \equiv 26 \mod 86 \iff 86|(100x - 26) \iff 100x - 26 = 86y' \iff 50x + 43y = 13$. First solve $50a + 43b = 1$ using the Euclidean Algorithm:

$$\begin{aligned} 50 &= 43 \times 1 + 7 \\ 43 &= 7 \times 6 + 1 \end{aligned}$$

and so

$$\begin{aligned} 1 &= 43 - 7 \times 6 \\ &= 43 - (50 - 43 \times 1) \times 6 \\ &= 7 \times 43 - 6 \times 50. \end{aligned}$$

We therefore take $a = -6$ and $b = 7$. We then set $x = 13a$, $y = -13b$ so that $50x + 43y = 13$. From this we can see that $x = -6 \times 13 = -78 \equiv 8 \mod 86$ is a solution, and that the general solution is $x_0 + \frac{n}{h}t = 8 + \frac{86}{2}t = 8 + 43t$.

Theorem 2.5 (Chinese Remainder Theorem (Sun-Tze, 3rd–4th century A.D.))**.** *Let $n_1, n_2, \ldots, n_t \in \mathbb{N}$ with $(n_i, n_j) = 1$ whenever $i \neq j$, (i.e. the n_i are "coprime in pairs") and let $a_1, a_2, \ldots, a_t \in \mathbb{Z}$ be given. Then there exists $x \in \mathbb{Z}$ such that $x \equiv a_i \mod n_i$ for all $i = 1, \ldots, t$. Moreover, if x' is any other solution, then $x' \equiv x \mod N$, where $N := n_1 n_2 \ldots n_t$.*

Proof. Define $N_i := N/n_i$. Then $(N_i, n_i) = 1$, since n_i is coprime to all the factors of N_i. Hence by Lemma 2.4 (or Lemma 2.3), there exists $x_i \in \mathbb{Z}$ such that $N_i x_i \equiv 1 \mod n_i$. Define $x = \sum_{i=1}^{t} a_i N_i x_i$. Thus $x \equiv a_k N_k x_k \mod n_k$ since $n_k | N_i$ for all $i \neq k$. Therefore $x \equiv a_k (N_k x_k) \equiv a_k \mod n_k$ for all k.

Also, if $x' \equiv a_k \mod n_k$ for all k, then $x' \equiv x \mod n_k$ for all k. Thus $n_k | (x' - x)$ for all k, and hence $n_1 n_2 \dots n_t | (x' - x)$, since the n_i are pairwise coprime. This yields $x' \equiv x \mod N$. □

Remark. We have used that $(n_i, n_j) = 1$ whenever $i \neq j$ twice in the above proof. This hypothesis is necessary because, for example, the pair of congruences $x \equiv 2 \mod 12$, $x \equiv 4 \mod 20$ has no solution.

Example. Solve:

$$\begin{aligned} x &\equiv 2 \mod 3, \\ x &\equiv 3 \mod 5, \\ x &\equiv 2 \mod 7. \end{aligned}$$

Following the proof, we put $N := 3 \times 5 \times 7 = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$ and

$$\begin{aligned} 35x_1 &\equiv 1 \mod 3 \implies \text{take } x_1 = 2, \\ 21x_2 &\equiv 1 \mod 5 \implies \text{take } x_2 = 1, \\ 15x_3 &\equiv 1 \mod 7 \implies \text{take } x_3 = 1. \end{aligned}$$

Therefore

$$x = 2N_1 x_1 + 3N_2 x_2 + 2N_3 x_3 = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) = 233,$$

and the smallest positive integer solution is $23 \equiv 233 \mod 105$.

Corollary 2.6. *If $m, n \in \mathbb{N}$ are coprime then*

(i) $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$,

(ii) $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. This result, sometimes also referred to as the Chinese Remainder Theorem, is from Part A Algebra. However, we give a sketch proof of part (i).

The isomorphism is given explicitly by

$$\phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

It is straightforward to check that this map is a well-defined homomorphism. It is onto by Theorem 2.5, and hence is injective by a counting argument. □

3 Polynomial Congruences

Theorem 3.1 (Wilson's Theorem, 1770)**.** *An integer $p \geq 2$ is prime if and only if $(p-1)! \equiv -1 \mod p$.*

Example. For $p = 5$, we have $(5-1)! = 4! = 24 \equiv -1 \mod 5$; but for $p = 6$, we have $(6-1)! = 5! = 120 \equiv 0 \mod 6$.

Proof. ($\Leftarrow$) If n is composite then there exists d dividing n with $1 < d < n$. Therefore $d|(n-1)!$ and $d|n$. So if $(n-1)! \equiv -1 \mod n$ then $n|((n-1)!+1)$ and so $d|((n-1)!+1)$. Hence $d|1 = ((n-1)!+1) - (n-1)!$. ※

($\Rightarrow$) One can easily check the cases $p = 2, 3$. Now assume p is prime with $p > 3$. Then by Lemma 2.3,

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{[a]_p \in \mathbb{Z}/p\mathbb{Z} : (a,p) = 1\} = \{[1]_p, [2]_p, \ldots, [p-1]_p\}.$$

Now look at those $[i]_p$ such that $[i]_p^2 = [1]_p$. For these values we have $i^2 \equiv 1 \mod p \Rightarrow p|(i^2-1) \Rightarrow p|(i-1)(i+1)$, and so $[i]_p = [1]_p$ or $[-1]_p$. Therefore, if we exclude these two cases, the remaining set $[2]_p, [3]_p, \ldots, [p-2]_p$ can be split into inverse pairs. It follows that $2 \times 3 \times 4 \times \ldots \times (p-2) \equiv 1 \mod p$, and hence that $(p-1)! \equiv -1 \mod p$. □

Theorem 3.2 (Fermat's Little Theorem, 1640)**.** *Let p be a prime and let $x \in \mathbb{Z}$ such that $p \nmid x$. Then $x^{p-1} \equiv 1 \mod p$.*

Proof. Let G be the group $(\mathbb{Z}/p\mathbb{Z})^\times$, so that $\#G = p-1$. Apply Lagrange's Theorem from group theory (see Mods), which implies that if G is a finite group and $g \in G$ then $g^{\#G} = i_G$. In our case we take $g = x + p\mathbb{Z}$, which gives

$$(x+p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z} \quad \Longrightarrow \quad x^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z} \quad \Longrightarrow \quad x^{p-1} \equiv 1 \mod p.$$

□

Alternative proof. We shall show that $x^p \equiv x \mod p$ for all $x \in \mathbb{N}$ (then it is true for all $x \in \mathbb{Z}$). This suffices because if $p \nmid x$ then

$$x^p \equiv x \mod p \quad \Longrightarrow \quad p|(x^p - x) \quad \Longrightarrow \quad p|x(x^{p-1}-1) \quad \Longrightarrow \quad p|(x^{p-1}-1),$$

(we have used that p is prime and $p \nmid x$ in the last step).

We proceed by induction on x. The case $x = 1$ is trivial. Suppose that $x^p \equiv x \mod p$ for some $x \in \mathbb{N}$. By the binomial theorem we have

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-1} + \ldots + \binom{p}{p-1}x + 1.$$

However, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p if $1 \leq k \leq p-1$ since $p|p!$ but $p \nmid k!$ and $p \nmid (p-k)!$. Therefore

$$(x+1)^p \equiv x^p + 1 \equiv x + 1 \mod p,$$

where the last equality uses the induction hypothesis. □

Remark. The converse to Fermat's Little Theorem is not always true. For example, $2^{340} \equiv 1 \mod 341$, but $341 = 11 \times 31$. Nonetheless, Fermat's Little Theorem provides a very useful necessary condition for primality: If n is odd, but $2^{n-1} \not\equiv 1 \mod n$, then n cannot be prime. In fact, if $2^{n-1} \equiv 1 \mod n$ then n is *probably* (but not necessarily) prime. Note that there are methods that can compute $2^{n-1} \mod n$ *very* rapidly.

Definition. For $n \in \mathbb{N}$ we define Euler's totient function, or the ϕ-function, by

$$\phi(n) := \#\{a \in \mathbb{N} : a \leq n, (a,n) = 1\} = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}.$$

Theorem 3.3 (Euler's Theorem, 1760)**.** *Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ with $(n,x) = 1$. Then $x^{\phi(n)} \equiv 1 \mod n$.*

Proof. Use Lagrange's Theorem from group theory exactly as before. □

Remark. Note that $\phi(p) = p-1$ for p prime, so that Euler's Theorem generalises Fermat's Little Theorem.

Lemma 3.4. *Let $n \in \mathbb{N}$.*

(i) If $n = p^e$ with p prime, then $\phi(n) = p^e - p^{e-1}$.

(ii) If $n = p_1^{e_1} \dots p_r^{e_r}$ with p_i distinct primes, then

$$\phi(n) = \phi(p_1^{e_1}) \dots \phi(p_r^{e_r}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. (i) If $n = p^e$ then for all m, either $(n,m) = 1$ or $p|m$. Thus

$$\begin{aligned} \phi(n) &= \#\{m \in \mathbb{N} : m \leq p^e, p \nmid m\} \\ &= \#\{m \in \mathbb{N} : m \leq p^e\} - \#\{m \in \mathbb{N} : m \leq p^e, p|m\} \\ &= p^e - p^{e-1}. \end{aligned}$$

(ii) Corollary 2.6 used repeatedly yields

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} = \left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right)^{\times} \times \left(\frac{\mathbb{Z}}{p_2^{e_2}\mathbb{Z}}\right)^{\times} \times \dots \left(\frac{\mathbb{Z}}{p_r^{e_r}\mathbb{Z}}\right)^{\times}.$$

Hence we have

$$\begin{aligned} \phi(n) &= \#\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} \\ &= \#\left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\right)^{\times} \times \#\left(\frac{\mathbb{Z}}{p_2^{e_2}\mathbb{Z}}\right)^{\times} \times \dots \times \#\left(\frac{\mathbb{Z}}{p_r^{e_r}\mathbb{Z}}\right)^{\times} \\ &= \phi(p_1^{e_1})\phi(p_2^{e_2}) \dots \phi(p_r^{e_r}) \\ &= (p_1^{e_1} - p_1^{e_1-1}) \dots (p_r^{e_r} - p_r^{e_r-1}) \\ &= p_1^{e_1} \dots p_r^{e_r} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

□

Lemma 3.5. *For any $n \in \mathbb{N}$ we have $\sum_{d|n} \phi(d) = n$.*

Proof. We classify integers $a \leq n$ according to their highest common factor with n. Thus

$$\{a \in \mathbb{N} : a \leq n\} = \bigcup_{d|n} \{a \in \mathbb{N} : a \leq n, (n,a) = d\} \quad \text{(disjoint union)}.$$

Hence $n = \sum_{d|n} S_d$ where $S_d := \#\{a \in \mathbb{N} : a \leq n, (n,a) = d\}$.

If $d|n$ then, by Lemma 1.5, we have $(n,a) = d \iff a = da'$ with $(\frac{n}{d}, a') = 1$. Moreover $a \leq n \iff a' \leq \frac{n}{d}$. It follows that

$$S_d = \#\{a' \in \mathbb{N}, a' \leq \tfrac{n}{d}, (\tfrac{n}{d}, a') = 1\},$$

and hence $S_d = \phi(\frac{n}{d})$. We deduce that $n = \sum_{d|n} \phi(\frac{n}{d})$. However when d runs over the divisors of n, so does $e = n/d$, so that $n = \sum_{e|n} \phi(e)$. □

Example. For $n = 12$ we have

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Theorem 3.6 (Lagrange's polynomial congruence theorem, 1768)**.** *Let $f(x) = a_0 + a_1 x \ldots + a_d x^d \in \mathbb{Z}[x]$ and let p be a prime with $p \nmid a_d$. Then $f(x) \equiv 0 \mod p$ has at most d solutions mod p.*

Remark. More generally, any polynomial equation of degree d over a field has at most d solutions (note that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field).

Proof. The proof is by induction on d. If x_0 is a root of $f(x) \equiv 0 \mod p$, we may write $f(x) = (x - x_0)q(x) + c$ by the Division Algorithm applied to the ring of polynomials. It follows that $f(x_0) = (x_0 - x_0)q(x_0) + c \equiv 0 \mod p$, whence $c \equiv 0 \mod p$. From this we see that $f(x) \equiv (x - x_0)q(x) \mod p$. Now the congruence $q(x) \equiv 0 \mod p$ has at most $d - 1$ roots, by the inductive hypothesis. Call these roots $x_1, x_2, \ldots, x_r$ with $r \leq d - 1$. Now, whenever $f(x^\star) \equiv 0 \mod p$ we have $(x^\star - x_0)q(x^\star) \equiv 0 \mod p$. Therefore $p|(x^\star - x_0)$ or $p|q(x^\star)$, and so $x^\star \equiv x_0 \mod p$ or $x^\star \equiv x_1, x_2, \ldots,$ or $x_r \mod p$. Hence there are at most d roots of the equation $f(x) \equiv 0 \mod p$. □

Example. Note that $x^2 - 1 \equiv 0 \mod 8$ has 4 roots, namely $1, 3, 5, 7 \mod 8$. This is not a counterexample to Theorem 3.6, however, because 8 is not prime (and $\mathbb{Z}/8\mathbb{Z}$ is not a field).

4 Primitive Roots

We investigate the structure of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Definition. Let $(a,n) = 1$ with $a, n \in \mathbb{N}$. Then the least $d \in \mathbb{N}$ such that $a^d \equiv 1 \mod n$ is called the order of $a \mod n$, and written $\mathrm{ord}_n(a)$. This is the order of $[a]_n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remark. Lagrange's Theorem in group theory tells us that the order of an element divides the order of the group; so $\mathrm{ord}_n(d)$ divides $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Definition. When $n \in \mathbb{N}$, we say that $a \in \mathbb{Z}$ is a primitive root of n if and only if $(a,n) = 1$ and $\mathrm{ord}_n(a) = \phi(n)$. This is equivalent to requiring a to be a generator for $(\mathbb{Z}/n\mathbb{Z})^\times$, which must therefore be cyclic.

Example. Let $n = 5$ and abbreviate $[x]_n = [x]_5$ to $[x]$. Then we have

$$[2]^0 = [1], \quad [2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [3], \quad [2]^4 = [16] = [1].$$

Therefore $\mathrm{ord}_5(2) = 4 = \phi(5)$ and so 2 is a primitive root of 5.

Remark. For some values of n there are no primitive roots. For example, every non-trivial element of $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ has order 2, and so $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic.

Lemma 4.1. *Let $n \in \mathbb{N}$.*

(i) $ord_n(a) = t \Rightarrow ord_n(a^u) = \frac{t}{(t,u)}$.

(ii) If r is a primitive root of n then r^u is too, if and only if $(u, \phi(n)) = 1$.

Proof. (i) Let $v = (t,u)$, and $t = vt'$, $u = vu'$ so that $(t', u') = 1$. We need to show that $\mathrm{ord}_n(a^u) = t'$. Note that

$$(a^u)^{t'} = a^{ut'} = a^{vu't'} = a^{tu'} = (a^t)^{u'} \equiv 1^{u'} \equiv 1 \mod n.$$

We now need to show that t' is minimal. Suppose that $(a^u)^s \equiv 1 \mod n$. Then, since t is the order of a, we must have that $t | us$. This implies that $t' | u's$, and hence $t' | s$, because t' and u' are coprime. Thus $t' \leq s$ as required.

(ii) This follows from part (i), since $\frac{\phi(n)}{(\phi(n),u)} = \phi(n) \iff (u, \phi(n)) = 1$.

□

Lemma 4.2. *Let p be prime and let d divide $p-1$. Then there are exactly $\phi(d)$ elements $a \mod p$ such that $ord_p(a) = d$. In particular, there are $\phi(p-1)$ primitive roots modulo p. Hence $(\mathbb{Z}/p\mathbb{Z})^\times$ is always cyclic.*

Proof. Let $d | (p-1)$ and write $\psi(d) = \#\{a \mod p : (a,p) = 1, \mathrm{ord}_p(a) = d\}$. We aim to show that $\psi(d) = \phi(d)$. By Lemma 3.5, $\sum_{d|(p-1)} \phi(d) = p-1$; and moreover, since $\mathrm{ord}_p(a) | (p-1)$, we must have $\sum_{d|(p-1)} \psi(d) = p-1$ (because there are $p-1$ possible $a \mod p$ with $(a,p) = 1$). If we can show that $\psi(d) \leq \phi(d)$ for all $d | (p-1)$ then $\psi(d) = \phi(d)$ for all such d. (Otherwise, if $\psi(d_0) < \phi(d)$ for some d_0, then $\sum_{d|(p-1)} \psi(d) < \sum_{d|(p-1)} \phi(d)$. ※). We examine two cases:

(i) $\psi(d) = 0$. Then $\psi(d) \leq \phi(d)$.

(ii) $\psi(d) \geq 1$. Then there exists a such that $(a, p) = 1$ and $\mathrm{ord}_p(a) = d$. By Lemma 4.1, $\mathrm{ord}_p(a^i)|d$ for all i. Moreover, $a^0, a^1, \ldots, a^{d-1}$ are all incongruent mod p since $\mathrm{ord}_p(a) = d$. Since $\mathrm{ord}_p(a^i)|d$, we have $(a^i)^d \equiv 1 \mod p$, so that the congruence $x^d - 1 \equiv 0 \mod p$ has at least d distinct roots mod p. By Theorem 3.6 (Lagrange's polynomial congruence theorem), there are at most d roots. Thus every root must be of the form $a^i \mod p$.

Now suppose that $\mathrm{ord}_p(b) = d$. Then $b^d \equiv 1 \mod p$ so that b is a root of the polynomial $x^d - 1 \equiv 0 \mod p$. Thus $b \equiv a^i \mod p$ for some i, which we may assume is in the range $0 \leq i < d$. Now we know that $\mathrm{ord}_p(b) = \mathrm{ord}_p(a^i) = \frac{d}{(d,i)}$ by Lemma 4.1. Hence $\mathrm{ord}_p(b) = d \Rightarrow (d, i) = 1$, so that

$$\psi(d) = \#\{a^i : 0 \leq i < d, (i, d) = 1\} = \phi(d).$$

Therefore $\psi(d) \leq \phi(d)$ as required. □

Theorem 4.3. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic $\Leftrightarrow$ n has a primitive root $\Leftrightarrow$ $n = 1, 2, 4, p^e, 2p^e$ where $e \in \mathbb{N}$ and p is an odd prime.*

Proof. Not examinable (but statement *is* examinable). See Baker, *A concise introduction to the theory of numbers*, §3.6, for example. □

Lemma 4.4. *Let $n \in \mathbb{N}$ and suppose that n has a primitive root. Let $a \in \mathbb{Z}$ with $(a, n) = 1$ and let $k \in \mathbb{N}$. Then*

$$\exists x \in \mathbb{Z} \text{ such that } x^k \equiv a \mod n \iff a^{\phi(n)/(\phi(n),k)} \equiv 1 \mod n.$$

Proof. Let g be a primitive root of n. Then $g^i \equiv g^j \mod n \iff \phi(n)|(i - j)$. For any $x \in \mathbb{Z}$ with $(x, n) = 1$, we define the discrete logarithm of x to base g modulo n by

$$g^{l(x)} \equiv x \mod n \text{ and } l(x) \in \{0, 1, \ldots, \phi(n) - 1\}.$$

Note that, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, there must be exactly one such value $l(x)$ for each x. Note too that $l(xy) \equiv l(x) + l(y) \mod \phi(n)$.

Now,

$$\begin{aligned}
\exists x \text{ such that } x^k \equiv a \mod n &\iff \exists x \text{ such that } (g^{l(x)})^k \equiv g^{l(a)} \mod n \\
&\iff \exists x \text{ such that } \phi(n)|(kl(x) - l(a)) \\
&\iff \exists x \text{ such that } kl(x) \equiv l(a) \mod \phi(n) \\
&\iff \exists z \text{ such that } kz \equiv l(a) \mod \phi(n) \\
&\iff (k, \phi(n))|l(a) \qquad \text{by Lemma 2.4} \\
&\iff \phi(n)|\frac{\phi(n)l(a)}{(\phi(n), k)} \\
&\iff g^{l(a)\phi(n)/(\phi(n),k)} \equiv 1 \mod n \\
&\iff a^{\phi(n)/(\phi(n),k)} \equiv 1 \mod n.
\end{aligned}$$

□

Remark. Lemma 4.4 does not hold without the hypothesis that n has a primitive root. For example, if $n = 8$, $k = 2$, $a = 3$ then there exists no $x \in \mathbb{Z}$ such that $x^2 \equiv 3 \mod 8$, yet $a^{\phi(8)/(\phi(8),2)} \equiv 3^{4/(4,2)} \equiv 3^2 \equiv 1 \mod 8$.

5 Quadratic Residues

Definition. Let p be an odd prime, and suppose we have $a \in \mathbb{Z}$ such that $p \nmid a$. Then a is a *Quadratic Residue* of p if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \mod p$, and a is *Quadratic Non-Residue* if not. We sometimes abbreviate these terms to "QR" and "QNR".

Definition. For any $a \in \mathbb{Z}$, we define the *Legendre Symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & p \nmid a \text{ and } a \text{ is a QR of } p, \\ -1, & p \nmid a \text{ and } a \text{ is a QNR of } p, \\ 0, & p|a. \end{cases}$$

Theorem 5.1 (Euler's Criterion)**.** *If p is an odd prime and $a \in \mathbb{Z}$ then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Proof. This is obvious if $p|a$. So suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \mod p$$

by Fermat's Little Theorem (Theorem 3.2). Hence

$$\begin{aligned} \left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p &\implies p \left| \left(a^{\frac{p-1}{2}}\right)^2 - 1 \right. \\ &\implies p \left| \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \right. \\ &\implies p \left| \left(a^{\frac{p-1}{2}} + 1\right) \text{ or } p \right| \left(a^{\frac{p-1}{2}} - 1\right) \\ &\implies a^{\frac{p-1}{2}} \equiv +1 \text{ or } -1 \mod p \end{aligned}$$

However, Lemma 4.4 yields

$$\begin{aligned} \left(\frac{a}{p}\right) = +1 &\iff \exists x \in \mathbb{Z} \text{ such that } x^2 \equiv a \mod p \\ &\iff a^{\frac{\phi(p)}{(\phi(p),2)}} \equiv 1 \mod p \\ &\iff a^{\frac{p-1}{2}} \equiv 1 \mod p. \end{aligned}$$

Therefore if $\left(\frac{a}{p}\right) = -1$, then the only possibility is that $a^{\frac{p-1}{2}} \equiv -1 \mod p$. $\square$

Lemma 5.2. *If p is an odd prime then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \mod 4, \\ -1, & p \equiv 3 \mod 4. \end{cases}$$

In other words, $x^2 \equiv -1 \mod p$ is soluble if and only if $p \equiv 1 \mod 4$.

Proof. By Euler's Criterion (Theorem 5.1) we have $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$, and both sides are $+1$ or -1. If they were different, we would have $+1 \equiv -1 \mod p$ and so $p|2$, which gives a contradiction as p is odd. □

Lemma 5.3. *Let p be an odd prime and $a, b \in \mathbb{Z}$.*

(i) $\left(\frac{1}{p}\right) = 1$*;*

(ii) if $a \equiv b \mod p$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *(periodicity);*

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *(multiplicativity) .*

Proof. Claims (i) and (ii) are trivial. For claim (iii), Euler's Criterion (Theorem 5.1) gives

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

But $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p$ implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, as in proof above. □

Example. Can we solve $x^2 \equiv 13 \mod 17$?

$$\begin{aligned} \left(\frac{13}{17}\right) &= \left(\frac{-4}{17}\right) && \text{by periodicity (Lemma 5.3(ii))} \\ &= \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right) && \text{by multiplicativity (Lemma 5.3(iii))} \\ &= \left(\frac{-1}{17}\right) && \text{as } (\pm 1)^2 = 1 \\ &= (-1)^{(17-1)/2} && \text{by Lemma 5.2} \\ &= (-1)^8 = 1 \end{aligned}$$

Hence the congruence is soluble! Note that this proof that a solution exists cannot be adapted to provide a concrete solution. It is purely an existence argument.

Lemma 5.4. *If p is an odd prime then there are $\frac{p-1}{2}$ incongruent QR's and $\frac{p-1}{2}$ incongruent QNR's. Equivalently, we have*

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Proof. Let g be a primitive root of p (such a g exists by Lemma 4.2). We have $\left(\frac{g}{p}\right) \equiv g^{(p-1)/2} \equiv \pm 1 \mod p$ by Euler's Criterion (Theorem 5.1). In fact, $g^{(p-1)/2} \equiv -1 \mod p$ since $\mathrm{ord}_p(g) = p-1$. We use the discrete logarithm $l(a)$ to base g as defined in the proof of Lemma 4.4. Then

$$\left(\frac{a}{p}\right) = \left(\frac{g^{l(a)}}{p}\right) = \left(\frac{g}{p}\right)^{l(a)} \equiv \left(g^{(p-1)/2}\right)^{l(a)} \equiv (-1)^{l(a)} \mod p.$$

Hence $\left(\frac{a}{p}\right) = (-1)^{l(a)}$ and so $\left(\frac{a}{p}\right) = +1$ if and only if $l(a)$ is even. However, $l(a)$ runs over $0, 1, 2, \ldots, p-2$ of which $\frac{p-1}{2}$ are even and $\frac{p-1}{2}$ are odd. □

Remark. Note that if p is an odd prime and g is a primitive root mod p, then

$$\begin{aligned} \{\text{quadratic residues mod } p\} &= \{g^0, g^2, g^4, \ldots, g^{p-3}\} \\ &= \{[1^2]_p, [2^2]_p, [3^2]_p, \ldots, [\left(\tfrac{p-1}{2}\right)^2]_p\}. \end{aligned}$$

Definition. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $\lambda(a, n)$ for the unique integer such that $a \equiv \lambda(a, n) \mod n$ and $0 \leq \lambda(a, n) < n$. (This is not a standard notation, and is intended merely for temporary use in our discussion of quadratic residues.)

Theorem 5.5 (Gauss's Lemma)**.** *Let p be an odd prime and let $a \in \mathbb{Z}$ with $a \nmid p$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\Lambda} \text{ where } \Lambda := \#\{j \in \mathbb{N} : 1 \leq j \leq \tfrac{p-1}{2}, \lambda(aj, p) > \tfrac{p}{2}\}.$$

Example. Let $p = 13$ and $a = 5$.
If $j = 1$ then $\lambda(aj, p) = \lambda(5, 13) = 5 < 13/2$.
If $j = 2$ then $\lambda(aj, p) = \lambda(10, 13) = 10 > 13/2$.
If $j = 3$ then $\lambda(aj, p) = \lambda(15, 13) = 2 < 13/2$.
If $j = 4$ then $\lambda(aj, p) = \lambda(20, 13) = 7 > 13/2$.
If $j = 5$ then $\lambda(aj, p) = \lambda(25, 13) = 12 > 13/2$.
If $j = 6$ then $\lambda(aj, p) = \lambda(30, 13) = 4 < 13/2$.
Hence $\Lambda = \#\{2, 4, 5\} = 3$ and so $\left(\frac{5}{13}\right) = (-1)^3 = -1$.

Proof. Let $S_a := \{aj : 1 \leq j \leq \frac{p-1}{2}\}$ and define

$$\{r_1, \ldots, r_m\} = \{\lambda(aj, p) : aj \in S_a,\ 0 < \lambda(aj, p) < \tfrac{p}{2}\},$$

$$\{s_1, \ldots, s_n\} = \{\lambda(aj, p) : aj \in S_a,\ \tfrac{p}{2} < \lambda(aj, p) < p\},$$

so that $n = \Lambda$. Note that $\lambda(aj, p) \neq \frac{p}{2}$ since $\frac{p}{2} \notin \mathbb{Z}$ and that $\lambda(aj, p) \neq 0$, since $p \nmid a$ and $p \nmid j$. Also note that if $j_1 \neq j_2$ then $\lambda(aj_1, p) \neq \lambda(aj_2, p)$ since

$$\begin{aligned} \lambda(aj_1, p) = \lambda(aj_2, p) &\implies aj_1 \equiv aj_2 \mod p \\ &\implies a(j_1 - j_2) \equiv 0 \mod p \\ &\implies j_1 - j_2 \equiv 0 \mod p \ \text{(since } p \nmid a\text{)}. \\ &\implies j_1 \equiv j_2 \mod p \\ &\implies j_1 = j_2 \ \text{(since } 0 < j_1, j_2 < p\text{)}. \end{aligned}$$

Hence $m+n = \#S_a = \frac{p-1}{2}$. We claim that

$$\{r_1, \ldots, r_m, (p-s_1), \ldots, (p-s_n)\} = \{1, 2, \ldots, \tfrac{p-1}{2}\}.$$

Clearly $r_i, (p-s_j) \in \{1, 2, \ldots, \frac{p-1}{2}\}$ and there are $\frac{p-1}{2}$ elements $r_i, (p-s_j)$, so it suffices to show that they are all different. We have already shown that $r_i \neq r_j$ and $s_i \neq s_j$ for $i \neq j$. To show that $r_i \neq p - s_j$ we argue by contradiction. If $r_i + s_j = p$, let $r_i = \lambda(aj_1, p)$ and $s_j = \lambda(aj_2, p)$. Then

$$r_i + s_j = p = \lambda(aj_1, p) + \lambda(aj_2, p) \equiv aj_1 + aj_2 \equiv a(j_1 + j_2) \mod p.$$

Hence $a(j_1 + j_2) \equiv 0 \mod p$. However $p \nmid a$ and $2 \leq j_1 + j_2 \leq p - 1$ so that $p \nmid (j_1 + j_2)$ ※. Therefore $r_i \neq p - s_i$, which proves the claim.

Finally,

$$\begin{aligned} r_1 r_2 \cdots r_m (p-s_1) \cdots (p-s_n) &= 1 \times 2 \times \cdots \times \tfrac{p-1}{2} = \left(\tfrac{p-1}{2}\right)! \\ &\equiv r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n (-1)^n \mod p. \end{aligned}$$

On the other hand, by the definition of r_i, s_j,

$$r_1 r_2 \cdots r_m s_1 s_2 \cdots s_n = \prod_{j=1}^{\frac{p-1}{2}} \lambda(aj, p) \equiv \prod_{j=1}^{\frac{p-1}{2}} (aj) = a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \mod p,$$

and hence

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^n a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \mod p.$$

Now, since $p \nmid \left(\frac{p-1}{2}\right)!$, we see that $1 \equiv (-1)^n a^{\frac{p-1}{2}} \mod p$. Thus $a^{\frac{p-1}{2}} \equiv (-1)^n \mod p$ and so $\left(\frac{a}{p}\right) \equiv (-1)^n \mod p$ by Euler's Criterion (Theorem 5.1). It therefore follows that $\left(\frac{a}{p}\right) = (-1)^n = (-1)^\Lambda$ as required. □

Corollary 5.6. *If p is an odd prime then*

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \mod 8, \\ -1, & p \equiv \pm 3 \mod 8. \end{cases}$$

Moreover,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. We shall apply Gauss's Lemma (Theorem 5.5) for $a = 2$, so that

$$\left(\frac{2}{p}\right) = (-1)^\Lambda \text{ where } \Lambda = \#\{1 \leq j \leq \left(\tfrac{p-1}{2}\right) : \lambda(2j, p) > \tfrac{p}{2}\}.$$

Note that $2j < \frac{p}{2}$ if $j < \frac{p}{4}$ and $\frac{p}{2} < 2j < p$ if $\frac{p}{4} < j < \frac{p}{2}$. It follows that $\Lambda = \#\{j \in \mathbb{N} : \frac{p}{4} < j < \frac{p}{2}\}$. We will now use the following standard notation:

Definition. For any $x \in \mathbb{R}$ we set $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \le x\}$. For example, $\lfloor 3 \rfloor = 3$, $\lfloor \pi \rfloor = 3$ and $\lfloor -\pi \rfloor = -4$.

With this notation we have

$$\#\left\{j : \tfrac{p}{4} < j < \tfrac{p}{2}\right\} = \#\left\{j \le \tfrac{p-1}{2}\right\} - \#\left\{j < \tfrac{p}{4}\right\} = \tfrac{p-1}{2} - \left\lfloor \tfrac{p}{4} \right\rfloor.$$

Now we look at cases:

(i) $p = 8k+1 \implies \frac{p-1}{2} = 4k,\ \lfloor \frac{p}{4} \rfloor = 2k \implies \Lambda = 2k,$

(ii) $p = 8k+3 \implies \frac{p-1}{2} = 4k+1,\ \lfloor \frac{p}{4} \rfloor = 2k \implies \Lambda = 2k+1,$

(iii) $p = 8k+5 \implies \frac{p-1}{2} = 4k+2,\ \lfloor \frac{p}{4} \rfloor = 2k+1 \implies \Lambda = 2k+1,$

(iv) $p = 8k+7 \implies \frac{p-1}{2} = 4k+3,\ \lfloor \frac{p}{4} \rfloor = 2k+1 \implies \Lambda = 2k+2.$

Hence $(-1)^\Lambda = +1 \iff p = 8k+1$ or $8k+7$. This proves the first assertion in the corollary.

To handle the second assertion we note that if $p = k + 8n$ then

$$\frac{p^2-1}{8} = \frac{k^2+16kn+64n^2-1}{8} = \frac{k^2-1}{8} + 2(kn+4n^2) \equiv \frac{k^2-1}{8} \mod 2.$$

By checking the cases $k = \pm 1, \pm 3$ we deduce that

$$\frac{p^2-1}{8} \equiv \begin{cases} 0 \mod 2, & p \equiv \pm 1 \mod 8, \\ 1 \mod 2, & p \equiv \pm 3 \mod 8, \end{cases}$$

and the result follows. □

Exercise. Use Theorem 5.5 to find $\left(\frac{-1}{p}\right)$ and hence recover Lemma 5.2.

Lemma 5.7. *Let p be an odd prime and let $a \in \mathbb{Z}$ with a odd and $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor ak/p \rfloor}.$$

Proof. Refer to the proof of Gauss's Lemma (Theorem 5.5) and recall that $\lambda(aj,p) \equiv aj \mod p$, with $0 \le \lambda(aj,p) < p$. Here $\lambda(aj,p) = aj - pk$ where $0 \le aj - pk < p$. It follows that $k \le \frac{aj}{p} < k+1$, and hence that $k = \left\lfloor \frac{aj}{p} \right\rfloor$. We therefore deduce that $\lambda(aj,p) = aj - p\left\lfloor \frac{aj}{p} \right\rfloor$. Using this expression we now have

$$\sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i = \sum_{j=1}^{(p-1)/2} \lambda(aj,p) = \sum_{j=1}^{(p-1)/2} \left(aj - p\left\lfloor \frac{aj}{p} \right\rfloor \right).$$

Hence, since a and p are odd, we have

$$\sum_{j=1}^{(p-1)/2} j - \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor \equiv \sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i \mod 2, \quad (*).$$

Recall from the proof of Gauss's Lemma (Theorem 5.5) that

$$\{r_1, \ldots, r_m, (p - s_1), \ldots, (p - s_n)\} = \{1, 2, \ldots, \tfrac{p-1}{2}\}.$$

Thus

$$\sum_{i=1}^{m} r_i + np + \sum_{i=1}^{n} s_i \equiv \sum_{j=1}^{(p-1)/2} j \mod 2,$$

and hence

$$\sum_{i=1}^{m} r_i + \sum_{i=1}^{n} s_i \equiv n + \sum_{j=1}^{(p-1)/2} j \mod 2.$$

Comparing this with $(*)$, we see that

$$n \equiv \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor \mod 2,$$

and the result follows from Gauss's Lemma (Theorem 5.5). □

Theorem 5.8 (The Law of Quadratic Reciprocity (Gauss, 1796))**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} = \begin{cases} +\left(\frac{q}{p}\right), & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4, \\ -\left(\frac{q}{p}\right), & \text{if } p \equiv q \equiv 3 \mod 4. \end{cases}$$

Remark. Gauss was particularly proud of this result, which he first proved at the age of 17. Indeed, he subsequently gave no fewer than seven further proofs. The theorem is remarkable, in that it connects the solubility of a congruence modulo p to the solubility of a second congruence to the seemingly unrelated modulus q.

One might ask whether there is an analogous theory for cubic residues, for example. One can indeed construct such a theory, but it naturally takes place in the ring $\mathbb{Z}[\omega]$ (where ω is a primitive cube root of unity) rather than in $\mathbb{Z}$.

Example. What is $\left(\frac{29}{53}\right)$? In other words, can we solve $x^2 \equiv 29 \mod 53$? Use LQR (the Law of Quadratic Reciprocity):

$$\begin{aligned} \left(\frac{29}{53}\right) &= \left(\frac{53}{29}\right) \quad \text{(by LQR since } 29 \equiv 1 \mod 4) \\ &= \left(\frac{24}{29}\right) \quad \text{(by periodicity since } 53 \equiv 24 \mod 29) \\ &= \left(\frac{2 \times 2 \times 2 \times 3}{29}\right) \\ &= \left(\frac{2}{29}\right)^3 \left(\frac{3}{29}\right) \quad \text{(by multiplicativity).} \end{aligned}$$

We now use LQR and Corollary 5.6 repeatedly:

$$\begin{aligned}
\left(\frac{2}{29}\right) &= -1 \quad \text{(by Corollary 5.6 since } 29 \equiv 3 \mod 8) \\
\left(\frac{3}{29}\right) &= \left(\frac{29}{3}\right) \quad \text{(by LQR since } 29 \equiv -3 \mod 4) \\
&= \left(\frac{2}{3}\right) \quad \text{(by periodicity since } 29 \equiv 2 \mod 3) \\
&= -1 \quad \text{(by Corollary 5.6 since } 3 \equiv 3 \mod 8).
\end{aligned}$$

Thus $\left(\frac{29}{53}\right) = (-1)^4 = +1$, and hence $x^2 \equiv 29 \mod 53$ is soluble.

Proof of Theorem 5.8. To prove the Law of Quadratic Reciprocity it suffices, by Lemma 5.7, to show that

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor = \frac{p-1}{2} \times \frac{q-1}{2}.$$

We will count the points in

$$R := \left\{(x,y) \in \mathbb{N} \times \mathbb{N} : 0 < x < \tfrac{p}{2},\, 0 < y < \tfrac{q}{2}\right\}$$

in two different ways:

(i) $\#R = \#\{x : 0 < x < \frac{p}{2}\} \times \#\{y : 0 < y < \frac{q}{2}\} = \frac{p-1}{2} \times \frac{q-1}{2}$ (since p and q are odd).

(ii) If a point (x,y) were on the line from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ we would have $y = \frac{qx}{p}$ and hence $py = qx$. However, then we would have $p|qx$, which is impossible, since $p \nmid q$ and $p \nmid x$ (recall that $0 < x < p/2$). Thus there are no points (x,y) of R on the line from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$.

How many points (x,y) of R are there below (or on) the diagonal? For each value of x with $1 \le x \le \frac{p-1}{2}$, the pairs (x,y) below the diagonal must satisfy $1 \le y \le \frac{q}{p}x$. However, there are $\lfloor \frac{qx}{p} \rfloor$ such values of y. It follows that the total number of points below (or on) the line $y = qx/p$ is

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor.$$

Similarly, there are

$$\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$$

points above (or on) the line. It follows that

$$\#R = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor.$$

Comparing the two expressions for $\#R$ gives the result. □

Theorem 5.9. *There are infinitely many primes p such that $p \equiv -1 \mod 8$.*

Proof. Suppose for a contradiction that there are only finitely many such primes, $p_1, \ldots, p_n$. Define $N := 8(p_1 \ldots p_n)^2 - 1$. Since N is odd and greater than 1 it must have at least one odd prime factor p, say. Then $(4p_1 \ldots p_n)^2 \equiv 2 \mod p$ and so $\left(\frac{2}{p}\right) = +1$. Thus $p \equiv \pm 1 \mod 8$, by Corollary 5.6. However, if $p \equiv -1 \mod 8$ then $p = p_i$ for some i. This is impossible, since $N \equiv -1 \mod p_i$, while $p|N$. Thus if $p|N$ then $p \equiv 1 \mod 8$. However, any product of primes of the form $1 \mod 8$ must itself be $1 \mod 8$. This implies that $N \equiv 1 \mod 8$, which is impossible, since $N = 8(p_1 \ldots p_n)^2 - 1$. ※ □

6 Factorisation

The factorisation of positive integers into their prime divisors is an ancient problem, and remains a difficult one even today. The modern use of coding systems based on the fact that factorisation is difficult make the issue one of considerable current interest. At the moment such systems use number of at least 200 decimal digits, and it is therefore numbers of this size that one would like to factor. Note that the problem of factorisation is much harder than primality testing.

Method 6.1 (Trial Division)**.** Let $n \in \mathbb{N}, n \geq 2$, then either n is prime or there exists a prime p dividing n such that $p \leq \sqrt{n}$. For a proof, assume n is composite, with $n = ab$ and $a, b \geq 2$. Without loss of generality, assume $a \leq b$. Then $a^2 \leq ab = n$ so that $a \leq \sqrt{n}$. Thus if p is any prime factor of a we have $p \leq \sqrt{n}$.

To use this method, test whether $2|n$, $3|n$, $5|n, \ldots$ for each prime up to $\sqrt{n}$. This is the best method for small n and is also a good method for a "random" n. However it may take up to $\sqrt{n}$ tests to prove or disprove primality of n.

Method 6.2 (Fermat's Method)**.** Let $n \in \mathbb{N}$ and let m be the least integer such that $m \geq \sqrt{n}$. Examine $m^2 - n, (m+1)^2 - n, \ldots$ looking for square values. If $(m+j)^2 - n = y^2$ say, then

$$n = (m+j)^2 - y^2 = (m+j+y)(m+j-y),$$

which gives a factorisation of n.

Note that if $n = ab$ with a, b odd and $a \leq b$ then

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \quad \text{with} \quad \frac{a \pm b}{2} \in \mathbb{Z}.$$

So this process does eventually find a factor because $m + j = \frac{a+b}{2}$, $y = \frac{a-b}{2}$ will work. Unfortunately, if n is prime, we have to check until $m + j = \frac{n+1}{2}$.

Example. Take $n = 6077$. Then $77 < \sqrt{6077} < 78$ so we start to look at $m = 78$, finding:

$$\begin{aligned} 78^2 - 6077 &= 7, \\ 79^2 - 6077 &= 164, \\ 80^2 - 6077 &= 323, \\ 81^2 - 6077 &= 484 = 22^2. \end{aligned}$$

Therefore $6077 = 81^2 - 22^2 = 103 \times 59$.

Remark. Fermat's method works best for $n = ab$ where a and b are close to each other.

Method 6.3 (Pollard's $p-1$ method)**.** This method is far more sophisticated. Let $n \in \mathbb{N}$ and suppose that $p|n$ where $(p-1)|k!$ for some "small" $k \in \mathbb{N}$. By Fermat's Little Theorem we have $2^{p-1} \equiv 1 \mod p$; and so if $(p-1)|k!$ then $2^{k!} \equiv 1 \mod p$. Thus $p|(2^{k!}-1)$, and if $p|n$ we get that $p|(2^{k!}-1, n)$.

We can now describe Pollard's algorithm. We compute $a_k \equiv 2^{k!} \mod n$ for $k = 1, 2, \ldots$, with $0 \leq a_k < n$. (We shall see below how to do this efficiently.) Then $(2^{k!}-1, n) = (a_k - 1, n)$ which we can compute easily using Euclid's Algorithm. If the answer is between 1 and n then it gives a factor of n. If n has a prime factor p with $(p-1)|k!$, we will have $p|(a_k - 1, n)$, so that the highest common factor will not merely be 1. (There is a danger though that the highest common factor will turn out to be n, in which case the method fails to find a factor of n. It transpires that the method breaks down in this way rather infrequently. However, in contrast to the first two approaches, Pollard's method does not always work.)

One can expect that this method is most successful when $p-1$ has only small prime factors. For example, $p = 2269$ would be discovered using $k = 9$ since

$$p - 1 = 2268 = 2^2 3^4 7 | 9!$$

How can we find a_k easily (and quickly)? We have $a_1 = 2$ and $a_k \equiv a_{k-1}^k \mod n$, since $a_{k-1}^k \equiv (2^{(k-1)!})^k \equiv 2^{(k-1)!k} \equiv 2^{k!} \mod n$. This process requires $k-1$ multiplications to find a_k, given a_{k-1}. Hence, by induction, we can compute a_k with $1 + 2 + \ldots + (k-1) = k(k-1)/2$ multiplications. This is far better than the naive process for computing $2^{k!} \mod n$ which would require $k! - 1$ multiplications!

Example. Let $n = 5419$ and find a factor by Pollard's $p-1$ method:

k	$a_k \mod 5917$	$(a_k, 5917)$
1	2	1
2	$2^2 = 4$	1 = (3,5917)
3	$4^3 = 64$	1 = (63,5917)
4	$64^4 \equiv 2521$	1 = (2520,5917)
5	$2521^5 \equiv 1648$	61 = (1647,5917)

Hence $n = 5917 = 61 \times 97$. Note that $61 - 1 = 2^2 \times 3 \times 5$ has only small prime factors.

7 Cryptography

Definition. In cryptography, the study of codes and ciphers, the *Plaintext* is the message to be encrypted, easily readable and completely insecure (e.g. a credit-card number, name and address), the *Ciphertext* is the message written in code (i.e. some horrible unreadable mess of numbers, symbols and letters). In order to move from the Plaintext to the Ciphertext, we must *encrypt* the Plaintext and to return to the Plaintext (in order to read the message once it has been received) we must *decrypt* it.

Many coding systems begin by translating a message written with ordinary letters into one involving numbers, using a standard system which is assumed to be well known to the sender, to the recipient, and to the enemy! One might use the standard ASCII codes, for example. We shall use the convention that we translate A to 00, B to 01, C to 02,..., and Z to 25. We will ignore all punctuation for simplicity. Thus CODE would be written in the numerical form 03140405, for example.

Method 7.1. A very basic cipher, dating from the times of the Romans, and used by Julius Caesar, is called the Caesar Cipher. To use this cipher, first pick a numerical "key" $1 \leq k \leq 25$ and translate each letter of the Plaintext to an integer from 00 to 25 as above. For each such integer P_i find $C_i \equiv P_i + k \mod 26$ in the same range $0 \leq C_i \leq 25$, and convert the C_i back into letters. One then sends the new string as the Ciphertext. In order to decrypt this code, one must repeat the algorithm but for each C_i in the Ciphertext, one computes $P_i \equiv C_i - k \mod 26$.

Example. Encrypt the string "TOP SECRET" using Caesar Shift with $k = 11$:

	T	O	P	S	E	C	R	E	T
P	19	14	15	18	04	02	17	04	19
C	04	25	00	03	15	13	02	15	04
	E	Z	A	C	P	N	B	P	E

Clearly, sending the message "EZA CPNBPE" wouldn't mean much to an onlooker, but to someone who knows how to reverse the algorithm, it tells him "TOP SECRET".

Remark. There are (at least) two problems with this system of encryption. Firstly, the sender and receiver both have to know the key number k. How can they agree on a value securely, other than by meeting in person? Secondly, if the enemy knows which type of system is being used, they can easily decrypt the message even without knowing k. After all, there are only 25 possible values to try! For 2000 years those who constructed codes focused on this second issue, without making any progress on the first difficulty.

Method 7.2. A substitution cipher is a more general version of the Caesar Cipher. This involves some permutation of the alphabet to encrypt messages, e.g. A $\mapsto$ E, B $\mapsto$ W, C $\mapsto$ U, ... There are 26! possible substitution ciphers.

However, this can be attacked using frequency analysis and suffers from the "secure key exchange" problem described above.

Method 7.3. The RSA Public Key Cryptosystem, invented by Rivest, Shamir and Adleman in 1977 allows messages to be sent securely without the need to exchange a "key" secretly. The letters RSA stand for the surnames of the three creators.

To model this system, let us call the sender of the message Alice and the intended recipient Bob. A malicious eavesdropper will appear later by the name of Eve. Bob chooses two large primes p and q and an integer e such that $(e, (p-1)(q-1)) = 1$. Typically p, q have hundreds of digits each. Bob announces e and $n = pq$ (but *not* the factors p and q) to the public. These are the "Public Key". When Alice wishes to send Bob a message securely, she converts her message to a numerical string P using the system above and looks up Bob's Public Key information. She then computes $C \equiv P^e \mod n$ and sends C to Bob. Now, Bob knows p and q so he can decrypt the message:

(i) Bob computes d such that $de \equiv 1 \mod (p-1)(q-1)$. He can do this using Euclid's Algorithm.

(ii) We have $C^d \equiv (P^e)^d = P^{ed} = P^{1+k(p-1)(q-1)} = P^{1+k\phi(n)}$ for some $k \in \mathbb{N}$, since $\phi(n) = \phi(pq) = (p-1)(q-1)$. By Theorem 3.3 (Euler's Theorem) we have $P^{\phi(n)} \equiv 1 \mod n$ so that $C^d \equiv P \mod n$.

(iii) Thus Bob can recover Alice's message by computing $C^d \equiv P \mod n$.

Note several important points:

(i) The primes p and q can be obtained by choosing random numbers in a suitable range and using efficient primality tests.

(ii) Actually, we need $(P, n) = 1$. It is possible for this to fail if $p|P$ or $q|P$ but since p, q are hundreds of digits long each, this is very unlikely indeed.

(iii) Alice's message P may be larger than n. In this case she will have to break P into pieces each of which is smaller than n and send them separately.

(iv) We need an efficient way of exponentiating mod n. One way to do this is as follows. Suppose we want to compute $m^r \mod n$ for some $m, r \in \mathbb{Z}$. Let $r_k \dots r_0$ be the binary expansion of r, so each r_i is either 0 or 1. We can inductively compute $m^{2^i} = (m^{2^{i-1}})^2 \mod n$ for $i = 1, \dots, k$. Then

$$m^r \equiv \prod_{i:r_i=1} m^{2^i} \mod n.$$

(v) Even with the above method, computing $P^e \mod n$ and $C^d \mod n$ are relatively slow jobs. For large P or C, even modern computers take a while to complete the algorithm. Thus a balance needs to be struck in choosing the size of n. If n is too small the code may be insecure (see below), but if n is too large the encryption/decryption processes may be impractically slow.

Example. Bob has published $e = 13$ and $n = 2537$ and Alice wishes to send him the very secret message "I love you". This produces $P = 0811142104241420$, but since she can only send messages of size below n so she has to break up her message into blocks 0811, 1421, 0424, 1420. She calculates $C \equiv P^{13} \mod 2537$ for each of them:

$$\begin{aligned}(0811)^{13} &\equiv 1542 \mod 2537,\\ (1421)^{13} &\equiv 0323 \mod 2537,\\ (0424)^{13} &\equiv 0467 \mod 2537,\\ (1420)^{13} &\equiv 2323 \mod 2537.\end{aligned}$$

So the Ciphertext is "1542032304672323" which she sends to Bob. Bob knows that $2537 = 43 \times 59$ so he finds a d such that $13d \equiv 1 \mod (42 \times 58)$. One such d is 937. Bob now calculates $P \equiv C^{937} \mod 2537$ for each block of four numbers:

$$\begin{aligned}(1542)^{937} &\equiv 0811 \mod 2537,\\ (0323)^{937} &\equiv 1421 \mod 2537,\\ (0467)^{937} &\equiv 0424 \mod 2537,\\ (2323)^{937} &\equiv 1420 \mod 2537.\end{aligned}$$

Hence Bob can read the message Alice sent him.

Can Eve, the eavesdropper, work out the secret message? One assumes she can intercept the encrypted version C—hacking into the email system is child's play these days. Moreover she will know n and e, which Bob has made public. Thus the problem is to find d. The only way we know to do this is by computing $\phi(n)$, for which she will need to find p and q. So the only known way to decrypt RSA messages requires one to factorise a number n of hundreds of digits. A large part of modern internet security is therefore based on the difficulty of the factorisation problem. There is however another important question— Is there another (quicker) way to find d?

We conclude by showing that finding $\phi(n)$ is tantamount to calculating p and q.

Lemma 7.4. *If we know n and $\phi(n)$ then we can easily calculate p and q.*

Proof. We have $\phi(n) = (p-1)(q-1) = n-p-q+1$ so that $p+q = n-\phi(n)+1$. Since also $pq = n$, the numbers p and q are roots of

$$x^2 - x(n - \phi(n) + 1) + n = 0.$$

Thus

$$p, q = \frac{1}{2}\left((n - \phi(n) + 1) \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}\right).$$

□