Number Theory

Henry Liu, 6 July 2007

1. Introduction

In one sentence, number theory is the area of mathematics which studies the properties of integers. Some of the most studied subareas are the theories of divisibility, prime numbers, and Diophantine equations (ie: equations whose solutions are integers, or maybe rational numbers).

Number theory is one of the oldest fields in mathematics, but yet as of today, it remains an area where many of the most famous questions in mathematics remain unsolved. Here are just two.

Conjecture 1 (Goldbach's Conjecture) *Every even integer ≥ 4 is the sum of two positive primes.*

Conjecture 2 (The Twin Primes Conjecture) *There are infinitely many twin primes. That is, there are infinitely many pairs (p, q), where p and q are positive primes, with $p + 2 = q$.*

On the other hand, there are many celebrated theorems in the area. Amongst them ...

Theorem 3 (The Prime Number Theorem) *For $n \in \mathbb{N}$, let $\pi(n)$ denote the number of positive prime numbers not exceeding n. Then, $\frac{\pi(n)\ln n}{n} \to 1$ as $n \to \infty$. In other words, as $n \to \infty$, we have $\pi(n)$ is approximately equal to $\frac{n}{\ln n}$.*

And very recently proved by Wiles in 1994 ...

Theorem 4 (Fermat's Last Theorem) *The Diophantine equation $x^n + y^n = z^n$ has no solutions, where $x, y, z, n \in \mathbb{Z}$ with $x, y, z \neq 0$ and $n \geq 3$.*

(Side note: In Conjectures 1, 2 and Theorem 3, we used the word "positive". We shall see soon that some negative integers can also be considered prime).

Questions and results like these are famous due to the simplicity of their statements, making them extremely appealing to a wide audience.

Number theory seems to be an area of mathematics which is frighteningly large. But outside of a typical school syllabus, not too much more ideas are actually needed at olympiad level. This set of notes aims to cover these very basic ideas. We shall prove some of the more interesting results whose proofs are manageable, and leave some others as exercises. The completion of a proof is denoted by the symbol $\square$.

2. Divisibility

2.1 Divisibility

Definition 1 *Let $a, b \in \mathbb{Z}$. We say that a* divides *b, written $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $ac = b$. If no such c exists, then we say that a* does not divide *b, and write $a \nmid b$*

Alternative ways of saying "a divides b" are:

- "a is a factor of b".
- "a is a divisor of b".
- "b is a multiple of a".
- "b is divisible by a".

Likewise for the negations.

Remark. Let $a \in \mathbb{Z}$. We have $a \mid 0$ for every a. Also, if $0 \mid a$, then $a = 0$ only.

Example 1. $-4 \mid 12$, and $5 \nmid 19$.

Definition 2 *Let $a \in \mathbb{Z} \setminus \{0\}$. Then*

- *a is a* unit *if $a = \pm 1$.*
- *a is a* prime number *if whenever $a = bc$, where $b, c \in \mathbb{Z}$, then either b or c is a unit.*
- *a is a* composite number *otherwise.*

In other words, the primes in $\mathbb{Z}$ are $\{\pm 2, \pm 3, \pm 5, \pm 7, \dots\}$, and the composites are $\{\pm 4, \pm 6, \pm 8, \pm 9, \dots\}$.

Finally, in many situations, we may want to restrict all of the above concepts to within $\mathbb{N}$ instead.

Now, we state some fairly trivial properties.

Proposition 5 *Let $a_1, \dots, a_n, b_1, \dots, b_n, a, b \in \mathbb{Z}$. We have the following.*

(a) If $a_1 \mid a_2$, $a_2 \mid a_3, \dots, a_{n-1} \mid a_n$, where $n \geq 2$, then $a_1 \mid a_n$.

(b) If $a \mid b_1, \dots, a \mid b_n$, then $a \mid x_1 b_1 + \cdots + x_n b_n$ for any $x_1, \dots, x_n \in \mathbb{Z}$.

(c) If $a_1 \mid b_1, \dots, a_n \mid b_n$, then $a_1 \cdots a_n \mid b_1 \cdots b_n$.

(d) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

(e) If $b \neq 0$ and $a \mid b$, then $a \leq |b|$.

Note that parts (a), (b) and (c) have useful special cases. For $a, b, c, d \in \mathbb{Z}$, we have the following.

(a′) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(b′) If $a \mid b$ and $a \mid c$, then $a \mid b \pm c$.

(c′) If $a \mid b$ and $c \mid d$, then $ab \mid cd$.

Proof of Proposition 5. See Exercise 1.

2.2 Highest Common Factors, Least Common Multiples

Definition 3 *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, not all zero. We say that $b \in \mathbb{Z}$ is a* common factor*, or a* common divisor*, of $a_1, a_2, \ldots, a_n$ if b divides a_i for each i. The largest such b is the* highest common factor*, or the* greatest common divisor*, of $a_1, a_2, \ldots, a_n$, and is denoted by* $\mathrm{hcf}(a_1, a_2, \ldots, a_n)$*, or* $\gcd(a_1, a_2, \ldots, a_n)$*, or just* $(a_1, a_2, \ldots, a_n)$*. We say that $a_1, a_2, \ldots, a_n$ are* relatively prime*, or* coprime*, if* $\mathrm{hcf}(a_1, a_2, \ldots, a_n) = 1$.

Definition 4 *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. We say that $b \in \mathbb{Z}$ is a* common multiple *of $a_1, a_2, \ldots, a_n$ if b is a multiple of a_i for each i. The smallest such b which is positive is the* least common multiple *of $a_1, a_2, \ldots, a_n$, and is denoted by* $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$*, or just* $[a_1, a_2, \ldots, a_n]$.

Remarks.

(a) $\mathrm{hcf}(a_1, a_2, \ldots, a_n)$ is well-defined if $a_i \neq 0$ for some i, but not so if $a_i = 0$ for every i (why?).

(b) Likewise, $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$ is well-defined if $a_i \neq 0$ for every i, but not so if $a_i = 0$ for some i (why?).

(c) In both definitions, the a_i are, in general, not necessarily pairwise distinct.

In advanced number theory, the least common multiple is generally much less studied than the highest common factor. Also, the case $n = 2$ seems to be considered more often.

Example 2. $\mathrm{hcf}(-18, 42) = 6$, $\mathrm{lcm}(-18, 42) = 126$.

For now, observe that two things are believable. Any common factor of $a_1, \ldots, a_n \in \mathbb{Z}$ ought to divide $\mathrm{hcf}(a_1, \ldots, a_n)$. Likewise, any common multiple of $a_1, \ldots, a_n \in \mathbb{Z}$ ought to be a multiple of $\mathrm{lcm}(a_1, \ldots, a_n)$. We shall come back to this a little later, as we need to develop some theory first.

We proceed by describing a method to show how to calculate the highest common factor of two integers (we shall return to discuss more integers a little later). We start with a fundamental result.

Theorem 6 (The Division Theorem) *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then, there exist unique $q, r \in \mathbb{Z}$, with $0 \leq r < |a|$, such that $b = qa + r$. Moreover, $r = 0$ if and only if $a \mid b$.*

Proof. See Exercise 2.

In Theorem 6, a is the *divisor*, b is the *dividend*, q is the *quotient*, and r is the *remainder*.

With Theorem 6, we can perform *Euclid's Algorithm* to find the highest common factor of two integers.

Theorem 7 (Euclid's Algorithm) *Let $a, b \in \mathbb{Z}$, with $a \neq 0$. If $a \mid b$, then $\mathrm{hcf}(a, b) = |a|$. Otherwise, $a \nmid b$, and there exist unique $q_1, \ldots, q_{n+1}, r_1, \ldots, r_n \in \mathbb{Z}$, with $0 < r_n < r_{n-1} < \cdots < r_1 < |a|$, such that*

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Moreover, we have $\mathrm{hcf}(a, b) = r_n$.
Note: If $n = 1$, then the equations will read

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1. \end{aligned}$$

Proof. If $a \mid b$, then certainly, $|a| \mid a$ and $|a| \mid b$. Now, if $x \mid a$ and $x \mid b$, then certainly $x \mid |a|$. By Proposition 5(e), this shows that $x \leq |a|$, so that $\mathrm{hcf}(a, b) = |a|$.

Otherwise, we apply Theorem 6 repeatedly. Apply Theorem 6 to a, b to get the first equation. We get $0 < r_1 < |a|$. Apply Theorem 6 to r_1, a to get the second equation. We get $0 \leq r_2 < r_1$. If $r_2 > 0$, apply Theorem 6 to r_2, r_1 to get the third equation. Repeating, we get a sequence of strictly decreasing remainders $r_1 > r_2 > \cdots$. This process must terminate; that is, after some n applications of Theorem 6, we must have a zero remainder. It is then clear that we get the equations in Theorem 7. Uniqueness is also clear, since each application of Theorem 6 yields a unique new equation.

We now prove that $\mathrm{hcf}(a, b) = r_n$. It is enough to prove (i) $r_n \mid a$ and $r_n \mid b$, and (ii) if $x \mid a$ and $x \mid b$, then $x \mid r_n$, because then by Proposition 5(e), we have $x \leq |r_n| = r_n$.

(i) The last equation shows that $r_n \mid r_{n-1}$. Then, the second last equation shows that $r_n \mid r_{n-2}$. Repeating, working upwards, the second equation shows that $r_n \mid a$, and finally, the first equation shows that $r_n \mid b$.

(ii) If $x \mid a$ and $x \mid b$, then the first equation shows that $x \mid r_1$. Then the second equation shows that $x \mid r_2$, and so on. Working downwards, we find that the second last equation shows that $x \mid r_n$, as required. □

Remark. If $b = 0$, then clearly $\mathrm{hcf}(a, b) = |a|$. Otherwise, when we apply the algorithm, we may assume that $|a| \leq |b|$, since if $|a| > |b|$, then the first equation in the algorithm yields $q_1 = 0$ and $r_1 = b$, so that the second equation will have us dividing b into a.

With Theorem 7, we have a method of finding the highest common factor of two integers.

Example 3. Use Euclid's Algorithm to find $\mathrm{hcf}(861, -672)$.
We apply the algorithm, starting by dividing -672 into 861. We have

$$\begin{aligned} 861 &= (-1) \times (-672) + 189 \\ -672 &= (-4) \times 189 + 84 \\ 189 &= 2 \times 84 + 21 \\ 84 &= 4 \times 21. \end{aligned}$$

We have $\mathrm{hcf}(861, -672) = 21$.

Euclid's Algorithm has many important consequences. One of them is *Bézout's Lemma*. We first give a definition.

Definition 5 *Let $a_1, \ldots, a_n, b \in \mathbb{Z}$. We say that b is a* linear combination *of the a_i if it can be represented in the form*

$$b = c_1 a_1 + \cdots + c_n a_n,$$

where $c_1, \ldots, c_n \in \mathbb{Z}$.

Theorem 8 (Bézout's Lemma) *Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $x, y \in \mathbb{Z}$ such that $\mathrm{hcf}(a, b) = xa + yb$. That is, $\mathrm{hcf}(a, b)$ is a linear combination of a and b.*

Proof. Throughout, let $h = \mathrm{hcf}(a, b)$.
If $a \mid b$, then $h = |a|$. We have $b = q_1 a$ for some $q_1 \in \mathbb{Z}$. If $a > 0$, then $h = a = (1 - q_1)a + b$. If $a < 0$, then $h = -a = (-1 - q_1)a + b$. So h is a linear combination of a and b.
Otherwise, $a \nmid b$, and Theorem 7 applies. Rewrite the equations (except the last)

as

$$\begin{aligned}
r_1 &= b - q_1 a \\
r_2 &= a - q_2 r_1 \\
r_3 &= r_1 - q_3 r_2 \\
&\vdots \\
r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3} \\
r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2} \\
r_n &= r_{n-2} - q_n r_{n-1}.
\end{aligned}$$

We have $h = r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2})$, so h is a linear combination of r_{n-2} and r_{n-3}. Repeating, we get h is a linear combination of r_{n-3} and r_{n-4}. Continue the process, we eventually get h as a linear combination of a and b. □

Indeed, Theorem 8 has a more general form.

Theorem 9 (Bézout's Lemma) *Let $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero. Then there exist $c_1, \ldots, c_n \in \mathbb{Z}$ such that $\mathrm{hcf}(a_1, \ldots, a_n) = c_1 a_1 + \cdots + c_n a_n$. That is, $\mathrm{hcf}(a_1, \ldots, a_n)$ is a linear combination of the a_i.*

Proof. See Exercise 3.

Example 4. Find hcf$(861, -672)$ as a linear combination of 861 and -672. We have $\mathrm{hcf}(861, -672) = 21$. Rewriting the equations,

$$\begin{aligned}
189 &= 861 - (-1) \times (-672) \\
84 &= -672 - (-4) \times 189 \\
21 &= 189 - 2 \times 84
\end{aligned}$$

We have

$$\begin{aligned}
21 &= 189 - 2[-672 - (-4) \times 189] = (-2) \times (-672) + (-7) \times 189 \\
&= (-2) \times (-672) + (-7)[861 - (-1) \times (-672)] \\
&= (-7) \times 861 + (-9) \times (-672).
\end{aligned}$$

As promised earlier, we can now prove the following.

Proposition 10 *Let $a_1, \ldots, a_n \in \mathbb{Z}$.*

(a) If $a_i \neq 0$ for some $1 \leq i \leq n$, and b is a common factor of the a_i, then $b \mid \mathrm{hcf}(a_1, \ldots, a_n)$.

(b) If $a_i \neq 0$ for every $1 \leq i \leq n$, and c is a common multiple of the a_i, then $\mathrm{lcm}(a_1, \ldots, a_n) \mid c$.

Proof. See Exercise 4.

Another consequence, this time from Bézout's Lemma, is the following proposition, often dismissed as trivial. It actually requires a rigourous proof.

Proposition 11 *Let $a_1, \ldots, a_n, p \in \mathbb{Z}$, with p prime. If $p \mid a_1 \cdots a_n$, then $p \mid a_i$, for some i.*

Proof. The assertion is trivial if $n = 1$. We prove the case $n = 2$. Suppose that $p \mid a_1 a_2$, and that $p \nmid a_1$. We shall show that $p \mid a_2$. We have $\text{hcf}(a_1, p) = 1$, since the largest factor of p is $|p|$, but clearly $|p| \nmid a_1$, and the next largest factor of p is 1, which is a factor of a_1. By Theorem 8, there exist $x, y \in \mathbb{Z}$ such that $1 = xa_1 + yp$. So, $a_2 = xa_1a_2 + ypa_2$. Since $p \mid a_1a_2$, clearly, $p \mid xa_1a_2 + ypa_2$. Hence $p \mid a_2$.

Now, we prove the result for $n \geq 3$. Suppose that $p \mid a_1 \cdots a_n$. By the result for $n = 2$, if $p \nmid a_1$, then $p \mid a_2 \cdots a_n$. Then, if $p \nmid a_2$, then $p \mid a_3 \cdots a_n$. Repeating this, clearly we will arrive at $p \mid a_i$, for some i. □

2.3 Unique Factorisation

We shall now discuss a key result in divisibility theory. We will see that every integer a with $|a| \geq 1$ can be factorised *uniquely* as a product of primes. The factorisation is unique up to ordering of the primes, and up to sign.

In practice, this result may seem obvious. Historically, mathematicians just took the result for granted. Euclid essentially gave a proof, but the great mathematician Gauss gave the first full correct proof.

Definition 6 *Let $a \in \mathbb{R} \setminus \{0\}$. We define the* sign function $\text{sgn}(a)$ *to be*

$$\text{sgn}(a) = \begin{cases} 1 & \text{if } a > 0, \\ -1 & \text{if } a < 0. \end{cases}$$

In some other situations, we may want to let $\text{sgn}(0) = 0$.

Theorem 12 (The Unique Factorisation Theorem) *Let $a \in \mathbb{Z}$ with $|a| \geq 1$. Then $a = (\text{sgn}(a))p_1 \cdots p_n$, where $p_1, \ldots, p_n > 0$ are primes, unique up to ordering.*

Remarks.

(a) The above unique factorisation of a is the *prime factorisation of a.*

(b) Of course, the primes may repeat. It is more common to write the prime factorisation as $a = (\text{sgn}(a))p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where $p_1, \ldots, p_n > 0$ are distinct primes, and $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. In some situations, we may want to change the restrictions, for example, allowing $\alpha_i = 0$, or, insisting that $p_1 < \cdots < p_n$.

(c) We also allow the empty product (with no primes!), which is defined to be 1. This allows for the case $a = \pm 1$.

Proof of Theorem 12. It is enough to prove the theorem for $a \geq 2$, since the third remark above dealt with $a = \pm 1$, and if $a \leq -2$, then a has a unique factorisation follows from that $-a \geq 2$ has a unique factorisation.

So, let $a \geq 2$. The proof is carried out in two parts: the existence and the uniqueness of the prime factorisation of a.

Existence. We do this part by induction on a. The result is clear for $a = 2$: 2 is a prime factorisation of 2. Now, let $a \geq 3$, and suppose that every integer b with $2 \leq b < a$ is a product of positive primes. If a is prime, then a has a prime factorisation a. Otherwise, a is composite, so it has a factorisation $a = cd$, where $2 \leq c, d < a$. By induction, both c and d can each be expressed as a product of positive primes. Multiplying these two products then gives a as a product of positive primes.

Uniqueness. Suppose that we have an integer $a \geq 2$ which can be expressed as a product of positive primes in two different ways. Dividing out any common primes, we have an equation of the form

$$p_1 \cdots p_r = q_1 \cdots q_s,$$

where $p_1, \ldots, p_r, q_1, \ldots, q_s$ are positive primes, and $p_i \neq q_j$ for any $1 \leq i \leq r$, $1 \leq j \leq s$ (but otherwise, not necessarily all distinct). But this is impossible, since $p_1 \mid p_1 \cdots p_r = q_1 \cdots q_s$, so by Proposition 11, $p_1 \mid q_j$ for some j, meaning that $p_1 = q_j$, a contradiction. □

Example 5. $168 = 2^3 \cdot 3 \cdot 7$, $-2700 = (-1)2^2 \cdot 3^3 \cdot 5^2$. Each of these factorisations is unique.

Theorem 12 will be an extremely useful result. We leave the proofs of two useful consequences as Exercises 5 and 6. Theorem 12 is also undoubtedly useful for solving many olympiad style problems.

With Theorem 12 now proved, we end this section by discussing how to find the highest common factor and the least common multiple of any number of integers.

Theorem 13 *Let $a_1, \ldots, a_m \in \mathbb{Z} \setminus \{0\}$, and obtain the unique prime factorisation of each a_i (by Theorem 12). Suppose that $p_1, \ldots, p_n$ is the collection distinct positive prime numbers formed by taking all the primes involved in the factorisations. Write the a_i as the following prime factorisations (each one unique).*

$$\begin{aligned} a_1 &= (\operatorname{sgn}(a_1))p_1^{\alpha_{11}} \cdots p_n^{\alpha_{1n}} \\ a_2 &= (\operatorname{sgn}(a_2))p_1^{\alpha_{21}} \cdots p_n^{\alpha_{2n}} \\ &\vdots \\ a_m &= (\operatorname{sgn}(a_m))p_1^{\alpha_{m1}} \cdots p_n^{\alpha_{mn}}, \end{aligned}$$

where $\alpha_{ij} \in \mathbb{Z}$, $\alpha_{ij} \geq 0$ for every $1 \leq i \leq m$, $1 \leq j \leq n$. Then

(a) $\operatorname{hcf}(a_1, \ldots, a_m) = p_1^{\beta_1} \cdots p_n^{\beta_n}$*, where β_j is the minimum of $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{mj}$, for each $1 \leq j \leq n$.*

(b) $\mathrm{lcm}(a_1, \ldots, a_m) = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, *where* γ_j *is the maximum of* $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{mj}$, *for each* $1 \leq j \leq n$.

Remark. The condition $a_i \neq 0$ for every $1 \leq i \leq m$ is required for the application of Theorem 12. It is not much more interesting if we allow some $a_i = 0$. Indeed, suppose that $a_1, \ldots, a_k \neq 0$, and $a_{k+1}, \ldots, a_m = 0$. Then $\mathrm{hcf}(a_1, \ldots, a_m) = \mathrm{hcf}(a_1, \ldots, a_k)$ (why?), and we can apply Theorem 13 to $a_1, \ldots, a_k$ to find $\mathrm{hcf}(a_1, \ldots, a_m)$. Of course, we cannot even talk about the least common multiple if some $a_i = 0$.

Proof of Theorem 13.

(a) Let $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$. We prove (i) $b \mid a_i$ for every $1 \leq i \leq m$, and (ii) if $x \mid a_i$ for every $1 \leq i \leq m$, then $x \mid b$, which then implies $x \leq b$ by Proposition 5(e), and $b = \mathrm{hcf}(a_1, \ldots, a_m)$.

(i) Fix i, $1 \leq i \leq m$. For every $1 \leq j \leq n$, since $\beta_j \leq \alpha_{ij}$, we have $p_j^{\beta_j} \mid p_j^{\alpha_{ij}}$. By Proposition 5(c), we have $p_1^{\beta_1} \cdots p_n^{\beta_n} \mid p_1^{\alpha_{i1}} \cdots p_n^{\alpha_{in}}$. So, $b \mid |a_i|$, and hence, $b \mid a_i$.

(ii) Consider the prime divisors of x. We cannot have a prime q different from the p_i involved, otherwise we have $q \mid x$, $x \mid a_1$, so $q \mid a_1$, a contradiction. So we can write $x = (\mathrm{sgn}(x))p_1^{\delta_1} \cdots p_n^{\delta_n}$, where $\delta_j \in \mathbb{Z}$, $\delta_j \geq 0$ for $1 \leq j \leq n$. We claim that $\delta_j \leq \beta_j$ for every $1 \leq j \leq n$. Indeed, fix j, and choose i so that $\beta_j = \alpha_{ij}$. Since $p_j^{\delta_j} \mid x$ and $x \mid a_i$, we have $p_j^{\delta_j} \mid a_i$, and hence $kp_j^{\delta_j} = a_i = (\mathrm{sgn}(a_i))p_1^{\alpha_{i1}} \cdots p_n^{\alpha_{in}}$, for some $k \in \mathbb{Z}$. If p_j^{δ} is involved in the prime factorisation of k, where $\delta \in \mathbb{Z}$, $\delta \geq 0$, by unique factorisation, the powers of p_j must match, and we have $\delta + \delta_j = \alpha_{ij}$. Hence, $\delta_j \leq \delta + \delta_j = \alpha_{ij} = \beta_j$, as required.

Hence, we have $p_j^{\delta_j} \mid p_j^{\beta_j}$ for every $1 \leq j \leq n$, so Proposition 5(c) gives $p_1^{\delta_1} \cdots p_n^{\delta_n} \mid p_1^{\beta_1} \cdots p_n^{\beta_n}$. So $|x| \mid b$, and hence $x \mid b$, as required.

(b) Let $c = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$. We prove (i) $a_i \mid c$ for every $1 \leq i \leq m$, and (ii) if $a_i \mid y$ for every $1 \leq i \leq m$, then $c \mid y$, which then implies $c \leq |y|$ by Proposition 5(e), and $c = \mathrm{lcm}(a_1, \ldots, a_m)$.

(i) Fix i, $1 \leq i \leq m$. For every $1 \leq j \leq n$, since $\alpha_{ij} \leq \gamma_j$, we have $p_j^{\alpha_{ij}} \mid p_j^{\gamma_j}$. By Proposition 5(c), we have $p_1^{\alpha_{i1}} \cdots p_n^{\alpha_{in}} \mid p_1^{\gamma_1} \cdots p_n^{\gamma_n}$. So, $|a_i| \mid c$, and hence, $a_i \mid c$.

(ii) Firstly, we claim that $p_j \mid y$ for every $1 \leq j \leq n$. Indeed, fix j. Choose i, $1 \leq i \leq m$, such that $p_j \mid a_i$. Since $a_i \mid y$, we have $p_j \mid y$.

So, we can write $y = tp_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$, where $t, \varepsilon_j \in \mathbb{Z}$, with $\varepsilon_j \geq 1$, and $p_j \nmid t$, for every $1 \leq j \leq n$. We claim that $\varepsilon_j \geq \gamma_j$ for every $1 \leq j \leq n$. Indeed, fix j, and choose i so that $\gamma_j = \alpha_{ij}$. Since $a_i \mid y$, we have $\ell a_i = y$ for some $\ell \in \mathbb{Z}$, that is, $\ell(\mathrm{sgn}(a_i))p_1^{\alpha_{i1}} \cdots p_n^{\alpha_{in}} = tp_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$. If p_j^{α} is involved in the prime factorisation of ℓ, where $\alpha \in \mathbb{Z}$, $\alpha \geq 0$, by unique factorisation, the powers of p_j must match, and we have $\alpha + \alpha_{ij} = \varepsilon_j$. Hence, $\varepsilon_j = \alpha + \alpha_{ij} \geq \alpha_{ij} = \gamma_j$, as required.

Hence, we have $p_j^{\gamma_j} \mid p_j^{\varepsilon_j}$ for every $1 \leq j \leq n$, so Proposition 5(c) gives $p_1^{\gamma_1} \cdots p_n^{\gamma_n} \mid p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$. So $c \mid p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$, and since $p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n} \mid y$, this gives $c \mid y$ as required. □

In practice, Theorem 13 is very easy to apply.

Example 6. Find $\mathrm{hcf}(3780, 1288, -50700)$ and $\mathrm{lcm}(3780, 1288, -50700)$. Writing out the unique prime factorisations, we have

$$\begin{aligned} 3780 &= 2^2 \cdot 3^3 \cdot 5 \cdot 7 = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 13^0 \cdot 23^0, \\ 1288 &= 2^3 \cdot 7 \cdot 23 = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 13^0 \cdot 23^1, \\ -50700 &= (-1)2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^2 = (-1)2^2 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 13^2 \cdot 23^0. \end{aligned}$$

So by Theorem 13, $\mathrm{hcf}(3780, 1288, -50700) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 13^0 \cdot 23^0 = 28$, and $\mathrm{lcm}(3780, 1288, -50700) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 13^2 \cdot 23^1 = 146928600$.

3. Congruences

3.1 Congruences: Notation and Arithmetic

The theory of congruences can be thought as a different way of studying divisibility. With a convenient notation which was introduced by Gauss, the theory offers simpler ways to produce proofs.

Definition 7 *Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. Then, we write $a \equiv b \pmod{m}$ if and only if $a - b$ is a multiple of m. In other words, a and b have the same remainder upon division by m. We say that a* is congruent to *b*, modulo *m.*

Otherwise, if $a - b$ is not a multiple of m, we write $a \not\equiv b \pmod{m}$, and say that a is not congruent to *b*, modulo *m.*

The number m is called the modulus*.*

Remarks.

(a) Of course, it is enough to assume that $m \geq 1$. If we were to remove the condition $m \geq 1$ in Definition 7, then clearly the case $m = 0$ is not interesting. Also, since $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{-m}$, considering modulo m is exactly the same as considering modulo $-m$. So it is enough to consider $m \geq 1$.

(b) "Congruence", like ordinary equality, is "transitive". That is, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. So, when we describe a chain of congruences together, we only need to write "(mod m)" once. For example, the above can be written $a \equiv b \equiv c \pmod{m}$.

By Theorem 6, given $a, m \in \mathbb{Z}$, $m \geq 1$, a is always congruent to a *unique* $b \in \mathbb{Z}$, modulo m, with $0 \leq b < m$. This is often the preferred form.

Example 7. $36 \equiv -40 \pmod{19}$, and $56 \equiv 98 \pmod{6}$. In preferred form, we have $36 \equiv -40 \equiv 17 \pmod{19}$, and $56 \equiv 98 \equiv 2 \pmod{6}$.

Now, note that, given $m \in \mathbb{N}$, we can naturally partition $\mathbb{N}$ into m parts.

Definition 8 *Let $x, m \in \mathbb{Z}$, where $m \geq 1$. Then, the set $\overline{x} = \{x + km : k \in \mathbb{Z}\}$ is the* residue class *of x. So, $y \equiv x \pmod{m}$ if and only if $y \in \overline{x}$.*

So, given $m \in \mathbb{N}$, there are exactly m residue classes in total: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Now, we would like to talk about performing arithmetic under such number systems. It turns out that addition/subtraction and multiplication work very similarly to ordinary arithmetic with the real numbers.

Example 8. $-59 + 34 = -25 \equiv 5 \,(\mathrm{mod}\ 15)$, and $(-3) \times 16 = -48 \equiv 1 \,(\mathrm{mod}\ 7)$.

Moreover, we have the following properties.

Proposition 14 *Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 1$. We have the following.*

(a) If $a \equiv b \,(\mathrm{mod}\ m)$ and $c \equiv d \,(\mathrm{mod}\ m)$, then $a \pm c \equiv b \pm d \,(\mathrm{mod}\ m)$.

(b) If $a \equiv b \,(\mathrm{mod}\ m)$ and $c \equiv d \,(\mathrm{mod}\ m)$, then $ac \equiv bd \,(\mathrm{mod}\ m)$.

(c) If $a \equiv b \,(\mathrm{mod}\ m)$, then $ca \equiv cb \,(\mathrm{mod}\ m)$.

Proof. See Exercise 7.

On the other hand, division is more tricky. In ordinary arithmetic, division by a real number x (where $x \neq 0$) is the same as multiplication by x^{-1}. Note that x^{-1} has the property $xx^{-1} = 1$. So, in the world of modulo m, we want to ask the question: Given $a, m \in \mathbb{Z}$, $m \geq 1$, can we find $b \in \mathbb{Z}$ such that $ab \equiv 1 \,(\mathrm{mod}\ m)$? Such a b, of course, may or may not exist, depending on a and m. For example, b certainly cannot exist if $a = 0$. Also, there is no b such that $4b \equiv 1 \pmod{6}$. So, when does b exist? We have the following.

Proposition 15 *Let $a, m \in \mathbb{Z}$ with $m \geq 1$. Then we can find $b \in \mathbb{Z}$ such that $ab \equiv 1 \,(\mathrm{mod}\ m)$ if and only if $\mathrm{hcf}(a, m) = 1$. Moreover, if b exists, then it is unique up to modulo m. That is, if $ab_1 \equiv 1 \,(\mathrm{mod}\ m)$ and $ab_2 \equiv 1 \,(\mathrm{mod}\ m)$, then $b_1 \equiv b_2 \,(\mathrm{mod}\ m)$.*

Proof. If $\mathrm{hcf}(a, m) = 1$, then by Theorem 8, there exist $x, y \in \mathbb{Z}$ with $1 = xa + ym$. So, $xa \equiv 1 \,(\mathrm{mod}\ m)$, and we can take $b = x$.

Conversely, suppose we can find $b \in \mathbb{Z}$ with $ab \equiv 1 \,(\mathrm{mod}\ m)$. Then $ab + km = 1$ for some $k \in \mathbb{Z}$. If $d \mid a$ and $d \mid m$, then $d \mid ab + km = 1$, so $d = \pm 1$, and hence $\mathrm{hcf}(a, m) = 1$.

Finally, if $ab_1 \equiv 1 \,(\mathrm{mod}\ m)$ and $ab_2 \equiv 1 \,(\mathrm{mod}\ m)$, then $ab_1 b_2 \equiv b_2 \,(\mathrm{mod}\ m)$ and $ab_1 b_2 \equiv b_1 \,(\mathrm{mod}\ m)$. Hence, $b_1 \equiv b_2 \equiv ab_1 b_2 \,(\mathrm{mod}\ m)$. □

Definition 9 *Let $a, m \in \mathbb{Z}$ with $m \geq 1$. If $b \in \mathbb{Z}$ satisfies $ab \equiv 1 \,(\mathrm{mod}\ m)$, then b is an* inverse *of a.*

3.2 Linear Equations

Just like ordinary algebra with the real numbers, where we consider solving equations in an unknown variable, we want to do something similar with congruence equations. Our solutions will be residue classes. Having developed the concept of inverses, we can now solve linear congruence equations.

Example 9. Solve $8x \equiv 7 \pmod{11}$, where $x \in \mathbb{Z}$.

We find an inverse of $8 \pmod{11}$, whose existence is guaranteed by Proposition 15. Indeed, $8 \cdot 7 \equiv 1 \pmod{11}$. So, $7 \cdot 8x \equiv 7 \cdot 7 \pmod{11}$, so $x \equiv 49 \equiv 5 \pmod{11}$.

If we cannot invert, we may divide out a common factor.

Example 10. Solve $6x \equiv -26 \pmod{16}$, where $x \in \mathbb{Z}$.

We have $6x \equiv -26 \pmod{16} \iff 6x = 16k - 26$ for some $k \in \mathbb{Z} \iff 3x = 8k - 13$ for some $k \in \mathbb{Z} \iff 3x \equiv -13 \pmod{8}$. Since $3 \cdot 3 \equiv 1 \pmod{8}$, we have $3 \cdot 3x \equiv 3(-13) \pmod{8}$, so $x \equiv -39 \equiv 1 \pmod{8}$.

Next, we want to talk about solving simultaneous linear congruence equations. For this, we have a key theorem.

Theorem 16 (Chinese Remainder Theorem) *Let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise coprime, and $m = m_1 \cdots m_r$. Let $a_1, \ldots, a_r \in \mathbb{Z}$. Then, the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

have a unique solution, up to modulo m.

Proof. For each $1 \leq i \leq r$, we have $\mathrm{hcf}(m_i, m/m_i) = 1$. This is easy to see by considering the prime factorisations of m_i and m/m_i: there are no primes in common since $\mathrm{hcf}(m_i, m_j) = 1$ for each $j \neq i$. Hence, if $d \in \mathbb{Z}$, $|d| \geq 2$, divides m_i and m/m_i, then so must any of its prime factors, and this is not possible. Hence $d = \pm 1$, and $\mathrm{hcf}(m_i, m/m_i) = 1$.

Now by Proposition 15, we can find $b_i \in \mathbb{Z}$ such that $mb_i/m_i \equiv 1 \pmod{m_i}$. Also, $mb_i/m_i \equiv 0 \pmod{m_j}$ if $j \neq i$. So, if we define

$$x_0 = \sum_{i=1}^{r} \frac{mb_i a_i}{m_i},$$

we see that x_0 satisfies $x_0 \equiv a_i \pmod{m_i}$, for every $1 \leq i \leq r$.

Finally, if $x_1 \in \mathbb{Z}$ is also a solution to the simultaneous congruences, then $x_1 \equiv$

$a_i \equiv x_0 \pmod{m_i}$, for every $1 \leq i \leq r$. So, $x_1 - x_0 \equiv 0 \pmod{m_i}$ for every $1 \leq i \leq r$. Now $\mathrm{lcm}(m_1, \ldots, m_r) = m$. This can be seen by considering the prime factorisations of the m_i: since the m_i are pairwise coprime, no prime occurs in more than one factorisation, and the assertion follows from Theorem 13(b). By Proposition 10(b), we have $x_1 - x_0 \equiv 0 \pmod{m}$, and $x_1 \equiv x_0 \pmod{m}$. □

Example 11. Solve the simultaneous congruences:

$$\begin{aligned} x &\equiv 2 \pmod{6}, \\ x &\equiv -10 \pmod{7}, \\ x &\equiv 8 \pmod{11}. \end{aligned}$$

Since the moduli are pairwise coprime, Theorem 16 applies: we have a unique solution, modulo 462.

Our aim is to compute x_0 in the proof of Theorem 16. With $m_1 = 6$, $m_2 = 7$, $m_3 = 11$, $a_1 = 2$, $a_2 = -10$, $a_3 = 8$, we need to find b_1, b_2, b_3 first.

b_1 is an inverse of $m_2 m_3 = 77$, modulo 6. Since $77 \equiv -1 \pmod{6}$, we may take $b_1 = -1$.

b_2 is an inverse of $m_1 m_3 = 66$, modulo 7. Since $66 \equiv 3 \pmod{7}$, we may take $b_2 = 5$.

b_3 is an inverse of $m_1 m_2 = 42$, modulo 11. Since $42 \equiv -2 \pmod{11}$, we may take $b_3 = -6$.

So, we have

$$\begin{aligned} x_0 &= m_2 m_3 b_1 a_1 + m_1 m_3 b_2 a_2 + m_1 m_2 b_3 a_3 \\ &= 77(-1)2 + 66 \cdot 5(-10) + 42(-6)8 \\ &= -154 - 3300 - 2016 \\ &= -5470 \\ &\equiv 74 \pmod{462}. \end{aligned}$$

Hence, the solutions to the simultaneous congruences are $x \equiv 74 \pmod{462}$.

Theorem 16 is helpful in olympiad problems, and we will have at least one problem where the theorem will be handy.

3.3 Quadratic Residues and Equations

We would now like to consider congruence equations which involve squares.

Definition 10 *Let $a, m \in \mathbb{Z}$ with $m \geq 1$ and $\mathrm{hcf}(a, m) = 1$. Then a is a* quadratic residue, modulo *m, if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If the congruence has no solution, then a is a* quadratic non-residue, modulo *m.*

To find the quadratic residues modulo m, one can square $0, 1, 2, \ldots, m-1$, and the quadratic residues are the squares obtained which are coprime to m, and the non-residues are those integers coprime to m which are not congruent to any of the squares, modulo m. This calculation can be shortened by squaring $0, \pm 1, \pm 2, \ldots, \pm(m-1)/2$ if m is odd, and squaring $0, \pm 1, \pm 2, \ldots, \pm(m-2)/2, m/2$ if m is even.

Example 12. For $m = 7$, squaring $0, \pm 1, \pm 2, \pm 3$ and reducing, modulo 7, we get $0^2 \equiv 0 \pmod 7$, $(\pm 1)^2 \equiv 1 \pmod 7$, $(\pm 2)^2 \equiv 4 \pmod 7$, $(\pm 3)^2 \equiv 2 \pmod 7$. So the quadratic residues, modulo 7, are $1, 2, 4$; we discard 0 since it is not coprime to 7, and the non-residues are $3, 5, 6 \pmod 7$.

For $m = 12$, squaring $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, 6$ and reducing, modulo 12, we get $0^2 \equiv 0 \pmod{12}$, $(\pm 1)^2 \equiv 1 \pmod{12}$, $(\pm 2)^2 \equiv 4 \pmod{12}$, $(\pm 3)^2 \equiv 9 \pmod{12}$, $(\pm 4)^2 \equiv 4 \pmod{12}$, $(\pm 5)^2 \equiv 1 \pmod{12}$, $6^2 \equiv 0 \pmod{12}$. So the only quadratic residue, modulo 12, is 1; we discard $0, 4, 9$, since they are each not coprime to 12, and the non-residues are $5, 7, 11 \pmod{12}$; these are the other integers coprime to 12.

This same technique also allows us to solve quadratic congruences. For example, $x^2 \equiv 3 \pmod 5$ has no solutions, while $x^2 \equiv 9 \pmod{12}$ has two solutions, $x \equiv \pm 3 \pmod{12}$.

We can compute a table of values of $n^2 \pmod m$ for m small. Below, we do this for $2 \leq m \leq 13$ and $0 \leq n \leq m-1$.

		m											
		2	3	4	5	6	7	8	9	10	11	12	13
	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	1	1	1	1	1	1	1
	2		1	0	4	4	4	4	4	4	4	4	4
	3			1	4	3	2	1	0	9	9	9	9
	4				1	4	2	0	7	6	5	4	3
	5					1	4	1	7	5	3	1	12
n	6						1	4	0	6	3	0	10
	7							1	4	9	5	1	10
	8								1	4	9	4	12
	9									1	4	9	3
	10										1	4	9
	11											1	4
	12												1

With this, it is possible to solve equations involving squares where the variables can only be integers. We can consider such an equation in a certain modulus.

Example 13. Find all solutions to

$$2^m + 7 = n^2, \tag{1}$$

where m and n are positive integers.

We consider (1) in modulo 4. If $m \geq 2$, then $2^m + 7 \equiv 3 \pmod 4$. But the table shows that no square can be congruent to $3 \pmod 4$, so there are no solutions for $m \geq 2$.

It remains to consider $m = 1$. In this case, we have $n = 3$. So the only solution is $(m, n) = (1, 3)$.

Note that we can also use modulo 8: there are no solutions for $m \geq 3$ by a similar argument, and we then have to check for $m = 1, 2$.

To tackle similar problems, we can similarly consider a particular modulus. It may not be easy to decide which modulus, but the idea is that, the fewer squares in the modulus there are, the better. Looking at the table, two of the best moduli to work with when squares are present are modulo 4 and modulo 8. We easily have the following, extremely useful result, often used in olympiads.

Proposition 17 *Let $n \in \mathbb{Z}$. Then,*

(a) $n^2 \equiv 0 \pmod 4$ if n is even, and $n^2 \equiv 1 \pmod 4$ if n is odd, while $n^2 \equiv 2, 3 \pmod 4$ are impossible.

(b) $n^2 \equiv 0 \pmod 8$ if $n \equiv 0 \pmod 4$, $n^2 \equiv 4 \pmod 8$ if $n \equiv 2 \pmod 4$, and $n^2 \equiv 1 \pmod 8$ if n is odd, while $n^2 \equiv 2, 3, 5, 6, 7 \pmod 8$ are impossible.

Proof. Obvious from the table. □

Finally, looking back at the table suggests that, when m is an odd prime, the number of quadratic residues and non-residues are each $\frac{m-1}{2}$. This indeed is the case for every such prime.

Proposition 18 *Let $p > 0$ be an odd prime. Then, the number of quadratic residues and non-residues are each equal to $\frac{p-1}{2}$. Moreover, the quadratic residues are exactly $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.*

Proof. Note that the set of quadratic residues is obtained from $\left\{(\pm 1)^2, (\pm 2)^2, \ldots, \left(\pm \frac{p-1}{2}\right)^2\right\} = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$, so that there are at most $\frac{p-1}{2}$ of them. We show that no two of these are congruent modulo p. Otherwise, if $x_1^2 \equiv x_2^2 \pmod p$, where $1 \leq x_2 < x_1 \leq \frac{p-1}{2}$, then $(x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod p$, so $p \mid x_1 - x_2$ or $p \mid x_1 + x_2$ by Proposition 11. But this is impossible, since $1 \leq x_1 - x_2, x_1 + x_2 < p$. Hence, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are exactly the quadratic residues. The number of non-residues is then $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$. □

3.4 Fermat's Little Theorem, Euler's Theorem, and Wilson's Theorem

In order to tackle some of the more powerful results, we must develop some elementary tools. In this section, we shall discuss three of the most well-known results in congruence theory. Each one is a very useful result in olympiads.

We first discuss *Fermat's Little Theorem*, one of the most well-known results in number theory. The theorem comes in two, equivalent forms.

Theorem 19 (Fermat's Little Theorem) *Let $p > 0$ be prime, and $a \in \mathbb{Z}$.*

(a) We have $a^p \equiv a \pmod{p}$.

(b) If $\operatorname{hcf}(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Moreover, the statements of (a) and (b) are equivalent.

There are at least three different proofs of this famous result. Below, we give possibly the most well-known proof.

Proof of Theorem 19. Firstly, we show the equivalence. After we do this, it then suffices to prove part (a).

Assume (a), so that $a^p \equiv a \pmod{p}$. If $\operatorname{hcf}(a, p) = 1$, then by Proposition 15, a has an inverse modulo p. Multiplying both sides of $a^p \equiv a \pmod{p}$ by this inverse then clearly gives $a^{p-1} \equiv 1 \pmod{p}$, so (b) holds.

Now, assume (b), so that $a^{p-1} \equiv 1 \pmod{p}$ whenever $\operatorname{hcf}(a, p) = 1$. If we do have $\operatorname{hcf}(a, p) = 1$, then multiplying both sides of $a^{p-1} \equiv 1 \pmod{p}$ by a gives $a^p \equiv a \pmod{p}$. If on the other hand, we have $\operatorname{hcf}(a, p) \neq 1$, then we must have $\operatorname{hcf}(a, p) = p$, so that $a \equiv 0 \pmod{p}$. In this case, we also have $a^p \equiv a \pmod{p}$. So, (a) holds.

Now, it suffices to prove (a). The result is trivial if $a \equiv 0 \pmod{p}$, so assume that $a \not\equiv 0 \pmod{p}$, and hence, $\operatorname{hcf}(a, p) = 1$. Consider the numbers $a, 2a, \ldots, (p-1)a$. No two of these are congruent modulo p: if $ia \equiv ja \pmod{p}$ for $1 \leq i < j \leq p-1$, then, since a has an inverse modulo p (by Proposition 15), we get $i \equiv j \pmod{p}$, a contradiction. Also, none of them is congruent to $0 \pmod{p}$: if $ia \equiv 0 \pmod{p}$, then Proposition 11 gives that $p \mid i$ or $p \mid a$, neither of which is possible. It follows that $a, 2a, \ldots, (p-1)a$ are congruent to $1, 2, \ldots, p-1$, modulo p, in some order. So, multiplying $p-1$ congruences, we get $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Since $\operatorname{hcf}((p-1)!, p) = 1$, $(p-1)!$ has an inverse modulo p, and hence $a^{p-1} \equiv 1 \pmod{p}$. It follows that $a^p \equiv a \pmod{p}$. □

Example 14. Simplify $9^{118} \pmod{31}$ to preferred form.

We use version (b) of Theorem 19. We have $9^{30} \equiv 1 \pmod{31}$. So, $9^{120} = (9^{30})^4 \equiv 1^4 \equiv 1 \pmod{31}$. Since $9^{118}9^2 = 9^{120} \equiv 1 \pmod{31}$, we want to find an inverse for 9^2, modulo 31. Now, $9^2 = 81 \equiv -12 \pmod{31}$, so we want an inverse for -12. Since $(-12)(-13) = 156 \equiv 1 \pmod{31}$, it follows that we have -13 is an inverse for 9^2, modulo 31. Therefore, $9^{118}9^2(-13) \equiv -13 \pmod{31}$, so, $9^{118} \equiv -13 \equiv 18 \pmod{31}$.

Next, we consider *Euler's Theorem.* This is a generalisation of Fermat's Little Theorem. We need a definition first.

Definition 11 *Let $n \in \mathbb{N}$. We define $\phi(n)$ to be the number of positive integers not greater than n which are coprime to n. The function $\phi(n)$ is* Euler's totient function*.*

Theorem 20 (Euler's Theorem) *Let $a, m \in \mathbb{Z}$, with $m \geq 1$ and* $\text{hcf}(a, m) = 1$*. Then* $a^{\phi(m)} \equiv 1 \pmod{m}$*.*

Note that, since $\phi(p) = p - 1$ for any prime $p > 0$, Theorem 20 clearly implies Theorem 19.

Proof of Theorem 20. We can prove this result with a similar argument to the one used in the previous theorem. We leave this proof in Exercise 8.

We end this section with another well-known result, *Wilson's Theorem.*

Theorem 21 (Wilson's Theorem) *Let $p > 0$ be prime. Then* $(p-1)! \equiv -1 \pmod{p}$*.*

Proof. This theorem has a reasonably simple proof. See Exercise 9.

There will be problems where these three results can be useful.

3.5 Quadratic Reciprocity

Looking back at Section 3.3, we can easily see one major problem when we wish to solve a quadratic congruence equation: if the modulus is large. Using the approach in Section 3.3 would mean that the computation would take far too long. For example, how do we answer the question: "Is the congruence $x^2 \equiv 5 \pmod{103}$ solvable?".

In this section, we shall briefly look at the theory behind this, the theory of *quadratic reciprocity.*

Definition 12 *Let $p > 0$ be an odd prime, and $a \in \mathbb{Z}$. Then, the* Legendre Symbol $\left(\frac{a}{p}\right)$ *is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } \pmod{p}, \\ 0 & \text{if } a \equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic non-residue } \pmod{p}. \end{cases}$$

We shall aim to find ways which will enable us to compute $\left(\frac{a}{p}\right)$.

Theorem 22 *Let $a, b, p \in \mathbb{Z}$, where $p > 0$ is an odd prime. Then,*

(a) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$*,*

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*,*

(c) $\left(\frac{a^2}{p}\right) = 1$ *if* $\text{hcf}(a, p) = 1$*,*

(d) $\left(\frac{1}{p}\right) = 1$*, and* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$*.*

Proof. Parts (b) and (d) are instant from part (a), while part (c) either follows from part (b), or from part (a) via Theorem 19. So, it remains to prove part (a). This part is obvious if $a \equiv 0 \pmod p$.

If $\left(\frac{a}{p}\right) = 1$, then there exists $x \in \mathbb{Z}$ with $x^2 \equiv a \pmod p$. Clearly, $\mathrm{hcf}(x,p) = 1$; if not, we will have $\left(\frac{a}{p}\right) = 0$. So by Theorem 19, we have $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right)$ (mod p).

If $\left(\frac{a}{p}\right) = -1$, then, for every $1 \leq i \leq p-1$, it is easy to see that there exists a unique $1 \leq i' \leq p-1$ such that $ii' \equiv a \pmod p$ (Existence is guaranteed by Proposition 15, while uniqueness can be shown by a similar argument to the last part of Proposition 15). Moreover, since a is a quadratic non-residue, we have $i \neq i'$. Furthermore, if $1 \leq j \leq p-1$, $j \neq i$, and j' ($1 \leq j' \leq p-1$) is found likewise: $jj' \equiv a \pmod p$, then $j' \neq i'$ (As before, assuming $j' = i'$ would give $j = i$). Hence, multiplying the $\frac{p-1}{2}$ congruences of the form $ii' \equiv a \pmod p$ together and using Theorem 21, we have $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$. □

Part (a) can be used to derive a criterion which determines the number of solutions to $x^2 \equiv a \pmod p$, where $p > 0$ is an odd prime, and $\mathrm{hcf}(a,p) = 1$.

Theorem 23 (Euler's Criterion) *Let $a, p \in \mathbb{Z}$, where $p > 0$ is an odd prime, and* $\mathrm{hcf}(a,p) = 1$. *Then, $x^2 \equiv a \pmod p$ has two solutions or no solutions, according to $a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod p$.*

Proof. By Theorem 22(a), we have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv \pm 1 \pmod p$, since $\mathrm{hcf}(a,p) = 1$.

If $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, then $\left(\frac{a}{p}\right) = -1$, so $x^2 \equiv a \pmod p$ has no solutions.

If $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, then $\left(\frac{a}{p}\right) = 1$, and $x^2 \equiv a \pmod p$ has a solution. If x_1 is a solution, then so is $-x_1$, and $x_1 \not\equiv -x_1 \pmod p$. If there is another solution x_2 where $x_2 \not\equiv x_1 \pmod p$ and $x_2 \not\equiv -x_1 \pmod p$, then, $x_2^2 \equiv x_1^2 \equiv a \pmod p$, so that $(x_2 - x_1)(x_2 + x_1) \equiv x_2^2 - x_1^2 \equiv 0 \pmod p$. So, either $x_2 - x_1 \equiv 0 \pmod p$ or $x_2 + x_1 \equiv 0 \pmod p$, which is a contradiction. So, there are exactly two solutions in this case. □

With Theorem 22, we now aim to derive the two main results which will enable us to compute $\left(\frac{a}{p}\right)$. By part (b), it is enough to consider a to be prime. We first consider the case $a = 2$.

Theorem 24 (A Lemma of Gauss) *Let $p > 0$ be an odd prime. Then, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. In other words, $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod 8$, and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3$ (mod 8).*

So, Theorem 24 says that 2 is a square (mod p) $\Longleftrightarrow p \equiv \pm 1 \pmod 8$, and a non-square (mod p) $\Longleftrightarrow p \equiv \pm 3 \pmod 8$.

Proof of Theorem 24. We first prove the following lemma, also due to Gauss.

Let $a, p \in \mathbb{Z}$, where $p > 0$ is an odd prime, and $\operatorname{hcf}(a,p) = 1$. Let $p' = \frac{p-1}{2}$. Obtain the remainders when $a, 2a, \ldots, p'a$ are divided by p, and let n be the number of these reminders greater than $\frac{p}{2}$. Then $\left(\frac{a}{p}\right) = (-1)^n$.

So, let $r_1, \ldots, r_n$ be the above remainders larger than $\frac{p}{2}$, and $s_1, \ldots, s_m$ be those less than $\frac{p}{2}$, so that $n + m = p'$. Note that the r_i and s_j are distinct modulo p. We have $p - r_1, \ldots, p - r_n < \frac{p}{2}$. We claim that $p - r_i \neq s_j$ for every i, j. If $p - r_i = s_j$ for some i, j, then $p = r_i + s_j \equiv (R_i + S_j)a \pmod{p}$ for some R_i, S_j, so that $p \mid R_i + S_j$, since $p \nmid a$. But also, we have $0 < R_i + S_j < p$, which is a contradiction.

Hence,

$$p'! = (p - r_1) \cdots (p - r_n) s_1 \cdots s_m \equiv (-1)^n r_1 \cdots r_n s_1 \cdots s_m \equiv (-1)^n p'! a^{p'} \pmod{p}.$$

Since $\operatorname{hcf}(p'!, p) = 1$, we have $1 \equiv (-1)^n a^{p'} \equiv (-1)^n \left(\frac{a}{p}\right) \pmod{p}$, by Theorem 22(a). Hence, $\left(\frac{a}{p}\right) = (-1)^n$, and the lemma holds.

We now aim to show that, if $a = 2$, then $n \equiv \frac{p^2-1}{8} \pmod{2}$, which implies the theorem. For $k = 1, \ldots, p'$, we have $ka = p\lfloor \frac{ka}{p} \rfloor + r_i$ for some i, or $ka = p\lfloor \frac{ka}{p} \rfloor + s_j$ for some j. So,

$$\sum_{k=1}^{p'} ka = p \sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j. \tag{2}$$

Also,

$$\sum_{k=1}^{p'} k = \sum_{i=1}^{n} (p - r_i) + \sum_{j=1}^{m} s_j. \tag{3}$$

So, subtracting (3) from (2) gives

$$(a-1) \sum_{k=1}^{p'} k = p\Big(\sum_{i=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor - n \Big) + 2 \sum_{i=1}^{n} r_i. \tag{4}$$

Now, if $a = 2$, then $\lfloor \frac{ka}{p} \rfloor = 0$ for every $k = 1, \ldots, p'$. Since $\sum_{k=1}^{p'} k = \frac{p^2-1}{8}$, by considering (4) in modulo 2, we have $\frac{p^2-1}{8} \equiv -pn \pmod{2}$, and hence, $\frac{p^2-1}{8} \equiv n \pmod{2}$, as required. □

Now, we consider the case when $a \geq 3$ is prime. We have the following remarkable result of Gauss.

Theorem 25 (Gauss' Quadratic Reciprocity Law) *Let $p, q > 0$ be distinct odd primes. Then,*

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

In other words, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$, unless if $p \equiv q \equiv 3 \pmod{4}$, in which case, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$.

So, Theorem 25 says that, if at least one of p and q is congruent to 1 (mod 4), then the congruences $x^2 \equiv q \pmod{p}$ and $x^2 \equiv p \pmod{q}$ are either both solvable or both not solvable. If $p \equiv q \equiv 3 \pmod{4}$, then one of the congruences is solvable, and the other is not.

Proof of Theorem 25. Write $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$. We first show that, if $t_1 = \sum_{x=1}^{p'} \lfloor \frac{qx}{p} \rfloor$ and $t_2 = \sum_{y=1}^{q'} \lfloor \frac{py}{q} \rfloor$, then $\left(\frac{q}{p}\right) = (-1)^{t_1}$ and $\left(\frac{p}{q}\right) = (-1)^{t_2}$. We use the lemma of Gauss at the start of the proof of Theorem 24, taking $a = q$ and n as defined there. Then, $\left(\frac{q}{p}\right) = (-1)^n$. So, we want to show that $n \equiv t_1 \pmod{2}$. With the exact same calculations that gave equation (4), we have

$$(q-1)\sum_{x=1}^{p'} x \equiv p\Big(\sum_{x=1}^{p'} \Big\lfloor \frac{qx}{p} \Big\rfloor - n\Big) \pmod{2}. \tag{5}$$

Since p and q are odd, clearly, (5) implies that $n \equiv \sum_{x=1}^{p'} \lfloor \frac{qx}{p} \rfloor \equiv t_1 \pmod{2}$. The proof that $\left(\frac{p}{q}\right) = (-1)^{t_2}$ is exactly the same, by switching p and q.

Now, consider the grid $S = \{(x, y) : x, y \in \mathbb{Z}, 1 \le x \le p', 1 \le y \le q'\}$. Let $S_1 = \{(x, y) \in S : qx > py\}$ and $S_2 = \{(x, y) \in S : qx < py\}$. Note that S is a disjoint union of S_1 and S_2, since no $(x, y) \in S$ satisfies $qx = py$, otherwise, we can find a rational $0 < \alpha < 1$ with $\alpha p, \alpha q \in \mathbb{Z}$, giving that p and q have a common divisor greater than 1.

Now,

$$|S_1| = \sum_{x=1}^{p'} \Big\lfloor \frac{qx}{p} \Big\rfloor = t_1, \quad |S_2| = \sum_{y=1}^{q'} \Big\lfloor \frac{py}{q} \Big\rfloor = t_2,$$

so that $\frac{p-1}{2} \cdot \frac{q-1}{2} = |S| = |S_1| + |S_2| = t_1 + t_2$. Hence, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t_2}(-1)^{t_1} = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$, as required. □

Example 15. Are the following congruences solvable?

(a) $x^2 \equiv 5 \pmod{103}$.

(b) $x^2 \equiv 30 \pmod{103}$.

We just have to find $\left(\frac{5}{103}\right)$ and $\left(\frac{30}{103}\right)$, and we may use Theorems 22, 24 and 25 to help us.

(a) Since $5 \equiv 1 \pmod{4}$, we have $\left(\frac{5}{103}\right)\left(\frac{103}{5}\right) = 1$. Now, $\left(\frac{103}{5}\right) = \left(\frac{3}{5}\right) = -1$, since $x^2 \equiv 3 \pmod{5}$ is not solvable. So, $\left(\frac{5}{103}\right) = -1$, and $x^2 \equiv 5 \pmod{103}$ is not solvable.

(b) We have $\left(\frac{30}{103}\right) = \left(\frac{2}{103}\right)\left(\frac{3}{103}\right)\left(\frac{5}{103}\right)$. Since $103 \equiv -1 \pmod{8}$, we have $\left(\frac{2}{103}\right) = 1$. Since $3 \equiv 103 \equiv 3 \pmod{4}$, we have $\left(\frac{3}{103}\right)\left(\frac{103}{3}\right) = -1$. $\left(\frac{103}{3}\right) = \left(\frac{1}{3}\right) = 1$, since $x^2 \equiv 1 \pmod{3}$ is solvable, so $\left(\frac{3}{103}\right) = -1$. We already have $\left(\frac{5}{103}\right) = -1$. Hence, $\left(\frac{30}{103}\right) = 1(-1)(-1) = 1$, and $x^2 \equiv 30 \pmod{103}$ is solvable. Applying Theorems 22(a) and 23 shows that there are exactly two solutions.

4. Diophantine Equations

In this section, we discuss some well-known Diophantine equations. These are equations whose solutions are integers, maybe sometimes, rational numbers. Such equations usually involve at least two variables. These equations are named after the Greek mathematician Diophantus. We will also discuss a useful method to solve these equations, *Fermat's method of infinite descent.*

4.1 Two Squares and Four Squares Theorems

We want to know when a given positive integer can be written as a sum of certain number of perfect squares. Our first aim will be to characterise those integers which can be represented as a sum of two squares. Certainly, there are integers for which this is not possible; for example, 6 and 7. So, for which integers can this be done?

We shall prove the following characterisation of these integers, due to Fermat.

Theorem 26 (Fermat) *Let $n \in \mathbb{N}$, with prime factorisation*

$$n = 2^\alpha \prod_{p \equiv 1\,(\mathrm{mod} 4)} p^\beta \prod_{q \equiv 3\,(\mathrm{mod} 4)} q^\gamma. \tag{6}$$

Then, n can be written as a sum of two non-negative squares if and only if all the exponents γ are even.

To help us, we first consider the case when n is an odd prime, which itself is an interesting result.

Theorem 27 (Fermat) *Let $p > 0$ be an odd prime. Then, p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof. Since squares are congruent to 0 or 1 (mod 4) by Proposition 17(a), certainly, p cannot be written as a sum of two squares if $p \equiv 3 \pmod 4$. It remains to show that p can be written as a sum of two squares if $p \equiv 1 \pmod 4$.

By Theorem 22(d), $\left(\frac{-1}{p}\right) = 1$, so that there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$. Take such an $x \in \{1, \ldots, p-1\}$, and consider the set $S = \{(a,b) : a, b \in \mathbb{Z}$ and $0 \le a, b < \sqrt{p}\}$. If $k = \lfloor \sqrt{p} \rfloor$, then $|S| = (k+1)^2 > p$. Hence by the pigeonhole principle, there exist two distinct members of S, say, $(a_1, b_1), (a_2, b_2) \in S$, with $a_1 + b_1 x \equiv a_2 + b_2 x \pmod p$. Setting $u = a_1 - a_2$ and $v = b_2 - b_1$ (note that at least one of u, v is non-zero), we have $u \equiv vx \pmod p$, so $u^2 \equiv (vx)^2 \equiv -v^2 \pmod p$, hence $u^2 + v^2 \equiv 0 \pmod p$. Now, $-\sqrt{p} < u, v < \sqrt{p}$, so that $0 < u^2 + v^2 < 2p$. It follows that $u^2 + v^2 = p$, as required. □

Proof of Theorem 26. Firstly, suppose that when n is written in the expression (6), the exponents γ are all even. Using the identity $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$, we see that if x and y can each be written as a sum of two squares, then so can xy. Since $2 = 1^2 + 1^2$, $q^2 = q^2 + 0^2$ if $q \equiv 3 \pmod 4$, and Theorem 27 gives that any prime $p \equiv 1 \pmod 4$ is a sum of two squares, it follows that n too is a sum of two squares.

Now we prove the converse. Firstly, we claim that, if $q \equiv 3 \pmod 4$ is prime, and $q \mid u^2 + v^2$, then $q \mid u$ and $q \mid v$. Assume that $q \nmid u$. Then, there exists u' with $uu' \equiv 1 \pmod q$. Since $u^2 + v^2 \equiv 0 \pmod q$, we have $0 \equiv (u^2 + v^2)u'^2 \equiv 1 + (vu')^2 \pmod q$, so that $x^2 \equiv -1 \pmod q$ has a solution vu'. This contradicts Theorem 22(d) that $\left(\frac{-1}{q}\right) = -1$ if $q \equiv 3 \pmod 4$, proving the claim.

Now, suppose that there exists an $n \in \mathbb{N}$ which is the sum of two squares, and has a prime congruent to $3 \pmod 4$ with an odd exponent in its prime factorisation. Let n_0 be the smallest such integer, with $n_0 = a^2 + b^2$ for $a, b \in \mathbb{Z}$, and $q_0 \equiv 3 \pmod 4$ be a prime factor of n_0 with odd exponent γ_0. By the claim, we have $q_0 \mid a$ and $q_0 \mid b$, so that $q_0^2 \mid a^2 + b^2 = n_0$, hence $\gamma_0 \geq 3$. But then, the integer $\frac{n_0}{q_0^2}$ is smaller than n_0, has the integer representation $\frac{n_0}{q_0^2} = \left(\frac{a}{q_0}\right)^2 + \left(\frac{b}{q_0}\right)^2$, and the exponent of q_0 in the prime factorisation of $\frac{n_0}{q_0^2}$ is $\gamma_0 - 2$, which is also odd. This is a contradiction and we are done. □

Next, we want to know that for any $n \in \mathbb{N}$, at most how many squares do we need so that n is the sum of the squares? We see that $n = 7$ shows that three squares is insufficient (and indeed, the same is true whenever $n \equiv 7 \pmod 8$, by an easy application of Proposition 17(b)). The next remarkable result of Lagrange shows that four squares is sufficient for *every* n.

Theorem 28 (Lagrange) *Every integer $n \in \mathbb{N}$ can be written as the sum of four non-negative squares.*

The rather short and standard proof of Theorem 28 uses techniques from an area of number theory called *Geometry of Numbers.* This area utilises high dimensional linear algebra on integer lattices, and such a proof of Theorem 28 considers a certain 4-dimensional integer lattice. We shall not give such a proof here, but we give a longer, more elementary proof.

Proof of Theorem 28. We begin with the following identity, due to Euler.

$$\begin{aligned}(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) \;=\; & (ae+bf+cg+dh)^2\\ & +(af-be-ch+dg)^2\\ & +(ag+bh-ce-df)^2\\ & +(ah-bg+cf-de)^2. \qquad (7)\end{aligned}$$

This means that it suffices to prove the theorem for $n = p$, where p is an odd prime, since $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Next, let $p = 2r + 1$, $X = \{x^2 : x = 0, 1, \ldots, r\}$, and $Y = \{-y^2 - 1 : y = 0, 1, \ldots, r\}$. Then, by Proposition 18, we have, modulo p, the elements of X are exactly the quadratic residues, united with 0. So, $|X| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$. Similarly, $|Y| = \frac{p+1}{2}$. Moreover, $X \cap Y = \emptyset$, since X has non-negative elements and Y has negative elements. Hence, $X \cup Y$ has $\frac{p+1}{2} + \frac{p+1}{2} = p+1$ elements. By the pigeonhole principle, it follows that an element of X is congruent to an element of Y, modulo p, say, $x^2 \equiv -y^2 - 1 \pmod{p}$. So, $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{N}$. We have $k \geq 1$, and $kp \leq 2r^2 + 1 < (2r+1)^2 = p^2$, so $k < p$.

It follows that there exist $a, b, c, d, m \in \mathbb{Z}$ such that $mp = a^2 + b^2 + c^2 + d^2$, where $1 \leq m < p$. Choose m to be the smallest such integer. If $m = 1$, we are done. Otherwise, if $m > 1$, we shall find an $\ell \in \mathbb{N}$ with $1 \leq \ell < m$, and ℓp is also a sum of four squares, which will be a contradiction.

If m is even, then we claim that we can take $\ell = \frac{m}{2}$. We have that either none, or two, or all four of a, b, c, d are even. So without loss of generality, assume that $a - b \equiv c - d \equiv 0 \pmod{2}$. Then,

$$\frac{m}{2} \cdot p = \Big(\frac{a-b}{2}\Big)^2 + \Big(\frac{a+b}{2}\Big)^2 + \Big(\frac{c-d}{2}\Big)^2 + \Big(\frac{c+d}{2}\Big)^2.$$

If m is odd, then take integers $-\frac{m}{2} < e, f, g, h < \frac{m}{2}$ with

$$e \equiv a \pmod{m}, \quad f \equiv b \pmod{m}, \quad g \equiv c \pmod{m}, \quad h \equiv d \pmod{m}. \tag{8}$$

So, $e^2 + f^2 + g^2 + h^2 \equiv 0 \pmod{m}$. Let $e^2 + f^2 + g^2 + h^2 = \ell m$ for some integer $\ell \geq 0$. We claim that ℓ is a suitable integer. We have $e^2 + f^2 + g^2 + h^2 < m^2$, so $\ell < m$. Also, if $\ell = 0$, then $e = f = g = h = 0$, which implies that $mp = a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m^2}$. It follows that $m \mid p$, which contradicts $1 < m < p$. So, $1 \leq \ell < m$. Now consider the identity (7). The left hand side is equal to $\ell p m^2$. For the right hand side, by (8), we have,

$$ae + bf + cg + dh \equiv e^2 + f^2 + g^2 + h^2 \equiv 0 \pmod{m},$$

and

$$\begin{aligned} af - be - ch + dg &= (af - be) + (dg - ch) \equiv 0 \pmod{m}, \\ ag + bh - ce - df &= (ag - ce) + (bh - df) \equiv 0 \pmod{m}, \\ ah - bg + cf - de &= (ah - de) + (cf - bg) \equiv 0 \pmod{m}. \end{aligned}$$

So, the right hand side of (7) is divisible by m^2. Dividing the resulting expression by m^2, we find that ℓp can be represented as a sum of four squares, as required. □

4.2 Pythagorean Triples

The equation

$$x^2 + y^2 = z^2, \tag{9}$$

where $x, y, z \in \mathbb{Z}$, is one of the most well-known Diophantine equations. It is well-known that a solution to (9), where x, y, z are positive real numbers, corresponds to the side lengths of a right angled triangle, where z is the length of the hypothenuse: *Pythagoras' Theorem.* So, a solution to (9) is called a *Pythagorean triple.* Two of the most well-known Pythagorean triples are $(3,4,5)$ and $(5,12,13)$.

We can start by simplifying the problem of solving (9) a little.

Firstly, note that if $(x,y,z) = (x_0,y_0,z_0)$ is a solution, then so is (kx_0,ky_0,kz_0) for any $k \in \mathbb{Z}$. So, it is enough to seek solutions to (9) where $\text{hcf}(x,y,z) = 1$. Such a solution is called a *primitive Pythagorean triple.*

Next, it is also enough to restrict the study of (9) to $x,y,z \in \mathbb{N}$. This is fairly clear. If $x = 0$, then $(x,y,z) = (0,y_0,z_0)$, where $|y_0| = |z_0|$, is a solution. Likewise for $y = 0$. While if $z = 0$, then $x = y = 0$. Also, if $(x,y,z) = (x_0,y_0,z_0)$ is a solution, then changing the sign of any number of x_0,y_0,z_0 also gives a solution.

Theorem 29 below describes *every* solution to (9). Part (a) describes those solutions with the above restrictions, while part (b) describes every solution in the integers.

Theorem 29 *Consider the Diophantine equation*

$$x^2 + y^2 = z^2. \tag{10}$$

(a) If $x,y,z \in \mathbb{N}$, where $\text{hcf}(x,y,z) = 1$, then the solutions of (10) are given by

$$\{x,y\} = \{2mn, m^2 - n^2\}, \quad z = m^2 + n^2,$$

where $m,n \in \mathbb{N}$, $\text{hcf}(m,n) = 1$, $m > n$, and m and n have opposite parity. That is, these are all the positive primitive Pythagorean triples.

(b) If $x,y,z \in \mathbb{Z}$, then all the solutions to (10) can be obtained by multiplying a primitive Pythagorean triple by some $k \in \mathbb{Z}$, followed by changing the sign of any number of the three resulting integers. In addition,

$$\{x,y\} = \{0,a\}, \quad z = b,$$

where $a,b \in \mathbb{Z}$ and $|a| = |b|$, are also solutions.

Proof. By the remarks before the theorem, it suffices to prove part (a) only.

So, assume that x,y,z are as in part (a). We first claim that $\text{hcf}(x,y) = \text{hcf}(x,z) = \text{hcf}(y,z) = 1$. If $h = \text{hcf}(x,y) > 1$, then $h^2 \mid x^2 + y^2 = z^2$, so that $z^2 = kh^2$ for some $k \in \mathbb{N}$. By considering prime factorisations, we see that $k = \ell^2$ for some $\ell \in \mathbb{N}$, giving $z = \ell h$, so $h \mid z$, contradicting $\text{hcf}(x,y,z) = 1$. The exact same argument gives that $\text{hcf}(x,z) = \text{hcf}(y,z) = 1$.

Next, x and y cannot have the same parity. They are not both even since $\text{hcf}(x,y) = 1$. If they are both odd, then $x^2 + y^2 \equiv 2 \pmod 4$, but $z^2 \not\equiv 2 \pmod 4$ by Proposition 17(a). So without loss of generality, assume that x is even and y is odd. Then, $z^2 = x^2 + y^2$ is odd, so z is odd. So, we have the equation

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2},$$

where $\frac{x}{2}, \frac{z+y}{2}, \frac{z-y}{2} \in \mathbb{N}$.

Now, we claim that $\mathrm{hcf}\big(\frac{z+y}{2}, \frac{z-y}{2}\big) = 1$. If $g = \mathrm{hcf}\big(\frac{z+y}{2}, \frac{z-y}{2}\big) > 1$, then $g \mid \frac{z+y}{2} - \frac{z-y}{2} = y$, and $g \mid \frac{z+y}{2} + \frac{z-y}{2} = z$. This contradicts $\mathrm{hcf}(y, z) = 1$.

So, by Exercise 6 (see Section 5.1), we have $\frac{z+y}{2} = m^2$ and $\frac{z-y}{2} = n^2$ for some $m, n \in \mathbb{N}$, and clearly, $\mathrm{hcf}(m, n) = 1$, since $\mathrm{hcf}\big(\frac{z+y}{2}, \frac{z-y}{2}\big) = 1$. We can now easily see that $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$, $m > n$, and m, n have different parity. Part (a) follows. □

We will have at least one problem later which uses Theorem 29.

4.3 Pell's Equation

We are about to discuss a remarkable family of Diophantine equations: *Pell's equations.* These equations have been surprisingly useful in many olympiad style problems. This section features fairly advanced material, so we shall only have an introductory treatment, and not provide a proof of the main result: Theorem 30.

Definition 13 *Let $d \in \mathbb{N}$ with $d \geq 2$. Then d is* square-free *if it has no square factors greater than* 1.

We want to consider solutions to an equation of the form

$$x^2 - dy^2 = 1, \tag{11}$$

where $x, y, d \in \mathbb{Z}$, $x, y \geq 0$ and $d \geq 2$ is square-free. Such an equation belongs to a family of equations collectively known as *Pell's equations.*

With d fixed, the solutions to (11) are given by second-order recurrence relations in both x and y.

Theorem 30 *Consider the Diophantine equation*

$$x^2 - dy^2 = 1, \tag{12}$$

where $x, y, d \in \mathbb{Z}$, $x, y \geq 0$ and $d \geq 2$ is square-free. Then, with d fixed, the solutions to (12) arise as follows. The first, trivial solution is $(x_0, y_0) = (1, 0)$. If (x_1, y_1) is the next, first non-trivial solution, then all the solutions are given by (x_k, y_k), where for $k \geq 2$,

$$\begin{aligned} x_k &= 2ax_{k-1} - x_{k-2}, \\ y_k &= 2ay_{k-1} - y_{k-2}, \end{aligned}$$

where $a = x_1$.

So, the first few cases are as follows.

d	Equation	a	First four solutions
2	$x^2 - 2y^2 = 1$	3	$(1, 0), (3, 2), (17, 12), (99, 70)$
3	$x^2 - 3y^2 = 1$	2	$(1, 0), (2, 1), (7, 4), (26, 15)$
5	$x^2 - 5y^2 = 1$	9	$(1, 0), (9, 4), (161, 72), (2889, 1292)$
6	$x^2 - 6y^2 = 1$	5	$(1, 0), (5, 2), (49, 20), (485, 198)$
7	$x^2 - 7y^2 = 1$	8	$(1, 0), (8, 3), (127, 48), (2024, 765)$
10	$x^2 - 10y^2 = 1$	19	$(1, 0), (19, 6), (721, 228), (27379, 8658)$
11	$x^2 - 11y^2 = 1$	10	$(1, 0), (10, 3), (199, 60), (3970, 1197)$

Generalisations of equation (11) have also been studied. These include $x^2 - dy^2 = n$, where $x, y, d, n \in \mathbb{Z}$, $x, y, d \geq 0$ and d is square free. In particular, the case $n = -1$ presents much interest, and is closely related to (11). Even more generally, $cx^2 - dy^2 = n$, where $x, y, c, d, n \in \mathbb{Z}$, with $x, y, c, d \geq 0$ and c, d square free, has been studied.

We now give an example of a problem where Theorem 30 can be used.

Example 16. This problem appeared in the British Mathematical Olympiad, Round 1, 2006/7. This was the final problem on the exam, and Theorem 30 can be used.

Let n be an integer. Show that, if $2 + 2\sqrt{1 + 12n^2}$ is an integer, then it is a perfect square.

Note that we may assume that $n \geq 0$. Firstly, we must have $1 + 12n^2 \geq 1$ is a perfect square, say, $1 + 12n^2 = m^2$, where $m \in \mathbb{N}$. If not, then let $1 + 12n^2 = t \geq 1$, where the prime factorisation of t has a prime with an odd power. We have $2^2 t = z^2$ for some $z \in \mathbb{Z}$. This is impossible since the prime factorisation of $2^2 t$ also has an odd prime power, but that of z^2 does not.

Now, we have $m^2 - 3(2n)^2 = 1$. This is a form of Pell's equation with $d = 3$ above. The solutions of $x^2 - 3y^2 = 1$ are given by the pairs (x_k, y_k), where x_k, y_k are generated by the recurrence relations

$$\begin{aligned} x_0 &= 1, x_1 = 2, x_k = 4x_{k-1} - x_{k-2} \text{ for } k \geq 2, \\ y_0 &= 0, y_1 = 1, y_k = 4y_{k-1} - y_{k-2} \text{ for } k \geq 2, \end{aligned}$$

giving the successive solutions $(x, y) = (1, 0), (2, 1), (7, 4), (26, 15), (97, 56), \ldots$. Looking at $m^2 - 3(2n)^2 = 1$ suggests that we must seek solutions to $x^2 - 3y^2 = 1$ where y is even. The recurrence $y_k = 4y_{k-1} - y_{k-2}$ easily shows that y_k and y_{k-2} have the same parity, and since y_0 is even and y_1 is odd, it follows that y_k is even if and only if k is even. It follows that the solutions for m are precisely x_k, where k is even. So it is a good idea to derive a recurrence relation for x_k, with k even. For $k \geq 4$, we have

$$\begin{aligned} x_k &= 4x_{k-1} - x_{k-2} = 4(4x_{k-2} - x_{k-3}) - x_{k-2} \\ &= 15x_{k-2} - 4x_{k-3} = 15x_{k-2} - (x_{k-2} + x_{k-4}) \\ &= 14x_{k-2} - x_{k-4}, \end{aligned}$$

since $4x_{k-3} = x_{k-2} + x_{k-4}$. It follows that the solutions to m are m_k, given by the recurrence relation

$$m_0 = 1, m_1 = 7, m_k = 14m_{k-1} - m_{k-2} \text{ for } k \geq 2,$$

giving the solutions $m = 1, 7, 97, 1351, \ldots$. We are done if we can show that for every term m_k of this sequence, $2 + 2m_k$ is a perfect square.

Now, observe that we have the pattern

$$\begin{aligned} m_0 &= 1 = 2 \cdot 1^2 - 1 = 2x_0^2 - 1, \\ m_1 &= 7 = 2 \cdot 2^2 - 1 = 2x_1^2 - 1, \\ m_2 &= 97 = 2 \cdot 7^2 - 1 = 2x_2^2 - 1. \end{aligned}$$

So, it is reasonable to claim that we have $m_k = 2x_k^2 - 1$ for every k. We prove this by induction on k. $m_k = 2x_k^2 - 1$ holds for $k = 0, 1$. For $k \geq 2$, assume that $m_\ell = 2x_\ell^2 - 1$ for every $0 \leq \ell < k$. We have

$$m_k = 14m_{k-1} - m_{k-2} = 14(2x_{k-1}^2 - 1) - (2x_{k-2}^2 - 1) = 28x_{k-1}^2 - 2x_{k-2}^2 - 13.$$

We would like this to be equal to $2x_k^2 - 1$. We have

$$2x_k^2 - 1 = 2(4x_{k-1} - x_{k-2})^2 - 1 = 32x_{k-1}^2 + 2x_{k-2}^2 - 16x_{k-1}x_{k-2} - 1,$$

so it suffices to show that

$$28x_{k-1}^2 - 2x_{k-2}^2 - 13 = 32x_{k-1}^2 + 2x_{k-2}^2 - 16x_{k-1}x_{k-2} - 1,$$

or equivalently,

$$x_{k-1}^2 + x_{k-2}^2 - 4x_{k-1}x_{k-2} + 3 = 0. \tag{13}$$

(13) holds for $k = 2$; $x_1^2 + x_0^2 - 4x_1x_0 + 3 = 2^2 + 1^2 - 4 \cdot 2 \cdot 1 + 3 = 0$. Now, for $k \geq 3$, we have

$$\begin{aligned} x_{k-1}^2 + x_{k-2}^2 - 4x_{k-1}x_{k-2} + 3 &= (4x_{k-2} - x_{k-3})^2 + x_{k-2}^2 - 4(4x_{k-2} - x_{k-3})x_{k-2} + 3 \\ &= x_{k-2}^2 + x_{k-3}^2 - 4x_{k-2}x_{k-3} + 3, \end{aligned}$$

so repeating this calculation successively gives

$$\begin{aligned} x_{k-1}^2 + x_{k-2}^2 - 4x_{k-1}x_{k-2} + 3 &= x_{k-2}^2 + x_{k-3}^2 - 4x_{k-2}x_{k-3} + 3 \\ &= \cdots \\ &= x_1^2 + x_0^2 - 4x_1x_0 + 3 = 0 \end{aligned}$$

We have now shown that $m_k = 2x_k^2 - 1$ for every k. So, $2 + 2m_k = (2x_k)^2$, and we are done.

We will have several more problems where Theorem 30 will be useful.

4.4 Fermat's Method of Infinite Descent

We shall discuss another useful method to tackle Diophantine equations. It is a contradiction type method, called *Fermat's method of infinite descent.* The idea is, we are given a Diophantine equation in positive (or non-negative) integers x, y, $z, \dots$. We then show that, if the equation is true for $x = a_1, y = b_1, z = c_1, \dots$, then it is true for $x = a_2 < a_1, y = b_2 < b_1, z = c_2 < c_1, \dots$, and then for the same reason, the equation is true for $x = a_3 < a_2, y = b_3 < b_2, z = c_3 < c_2, \dots$, and so on. This cannot happen infinitely often, by the positivity of $x, y, z, \dots$.

It is best to illustrate this method by an example.

Example 17. *Show that the equation*

$$x^2 + y^2 + z^2 = 2xyz \tag{14}$$

has no solutions in non-negative integers x, y, z, other than $x = y = z = 0$.

Suppose that we can find a solution $(x, y, z) = (x_1, y_1, z_1)$, where at least one of x_1, y_1, z_1 is positive. The right hand side of (14) is even, hence so is the left hand side. So either x_1, y_1, z_1 are all even, or two of x_1, y_1, z_1 are odd and the other is even. For the latter case, by Proposition 17(a), the left hand side of (14) is congruent to $2 \pmod 4$, while the right hand side is congruent to $0 \pmod 4$; impossible. It follows that $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$ for some non-negative integers x_2, y_2, z_2, with at least one positive. Substituting these into (14), we find

$$x_2^2 + y_2^2 + z_2^2 = 4x_2y_2z_2. \tag{15}$$

Using (15) to apply a similar argument, we find that x_2, y_2, z_2 must all be even as well, so that x_1, y_1, z_1 are all multiples of 4. Repeating the argument successively, we find that x_1, y_1, z_1 are all divisible by as large a power of 2 as we like. This is impossible, unless if $x_1 = y_1 = z_1 = 0$.

5. Problems

We divide the problems into two parts. The first set consists of some elementary exercises; some of these exercises complete most of the missing proofs. The second set consists of the challenges.

5.1 Elementary Exercises

1. Prove Proposition 5.

2. Prove Theorem 6 as follows. Consider the set

$$\dots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \dots.$$

Letting r be the least non-negative member of this set, and letting $r = b - qa$, show that this choice of q and r satisfies the conditions of Theorem 6. Also, prove the "Moreover" part of the theorem.

3. Use the following guideline to prove Theorem 9. This is a different approach to the one used to prove Theorem 8, and so it is a second proof of Theorem 8 as well.

   Consider the linear combinations of the form

$$c_1 a_1 + \cdots + c_n a_n,$$

   as $c_1, \ldots, c_n$ vary over $\mathbb{Z}$. Observe that these linear combinations can take positive and negative values, as well as 0. So, choose $c_1', \ldots, c_n' \in \mathbb{Z}$ so that $c_1' a_1 + \cdots + c_n' a_n$ has the least positive value. Let $\ell = c_1' a_1 + \cdots + c_n' a_n$.

   (a) Prove that $\ell \mid a_i$ for every i as follows. Assume that $\ell \nmid a_i$. Use Theorem 6 to obtain a contradiction.

   (b) Let $h = \mathrm{hcf}(a_1, \ldots, a_n)$. Use some of the properties of Proposition 5 to show that $h = \ell$.

4. Prove Proposition 10 as follows.

   (a) Apply Theorem 9.

   (b) Use a contradiction argument, and apply Theorem 6.

5. Suppose that $z \in \mathbb{Z} \backslash \{0\}$, with prime factorisation $z = \mathrm{sgn}(z) p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where $p_i, \alpha_i \in \mathbb{N}$ and $p_i > 0$ is prime, for $1 \leq i \leq n$.

   (a) How many distinct divisors of z are there?

   (b) How many distinct positive divisors of z are there?

6. Suppose that $a, b \in \mathbb{Z}$ with $\mathrm{hcf}(a, b) = 1$. Prove that, if $|ab|$ is a perfect square, then so are $|a|$ and $|b|$.

7. Prove Proposition 14.

8. Prove Theorem 20 as follows. Let $b_1, \ldots, b_{\phi(m)}$ be those positive integers not greater than m, each of which is coprime to m. Consider the set $ab_1, \ldots, ab_{\phi(m)}$. Show that no two of these numbers are congruent modulo m, and that each one is coprime to m. Deduce Theorem 20 with a similar argument to the proof of Theorem 19.

9. Prove Theorem 21 as follows. Firstly, verify that the result holds for $p = 2, 3$. Now, assume $p \geq 5$. Prove the following.

   (a) For $a \in \mathbb{Z}$ and $p > 0$ prime, show that $a^2 \equiv 1 \pmod{p} \iff a \equiv \pm 1$ (mod p).

   (b) Show that for every $b \in \{2, 3, \ldots, p-2\}$, b has a unique inverse, modulo p, in $\{2, 3, \ldots, p-2\}$, which is distinct from b. Proposition 15 will help here.

(c) Deduce Theorem 21.

10. Prove that the equation $x^4 + y^4 = z^4$ has no solutions for $x, y, z \in \mathbb{N}$. This special case of Fermat's Last Theorem is one of Fermat's most famous results. Hints: Use infinite descent, and ideas from Theorem 29.

5.2. Olympiad Style Problems

Here are the more challenging problems. The ordering does not necessarily reflect the difficulty of the problems.

1. Find all solutions to the equation
$$5^x \cdot 7^y + 4 = 3^z,$$
where x, y, z are non-negative integers.

2. Let A be the sum of the digits of the decimal representation of 4444^{4444}. Let B be the sum of the digits of A. What is the sum of the digits of B?

3. Find the smallest integer $n > 1$ such that the average of $1^2, 2^2, 3^2, \ldots, n^2$ is itself a perfect square.

4. Find all solutions to the equation
$$x_1^4 + x_2^4 + \cdots + x_{14}^4 = 9999,$$
where $x_1, x_2, \ldots, x_{14} \in \mathbb{Z}$.

5. Let $m = \frac{1}{3}(4^p - 1)$, where p is a prime number with $p > 3$. Prove that 2^{m-1} has a remainder of 1 when divided by m.

6. Find all integers n such that $3^n + n^3$ is the cube of an integer.

7. For $a, b, c, d \in \mathbb{Z}$, prove that
$$(ab, cd) = (a, c)(b, d)\left(\frac{a}{(a, c)}, \frac{d}{(b, d)}\right)\left(\frac{c}{(a, c)}, \frac{b}{(b, d)}\right).$$

8. For $a, b, c \in \mathbb{Z}$, prove that
$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}.$$

9. Find all $n \in \mathbb{N}$ with the property that, if the leading digit of the decimal expansion of 2^n is removed, the resulting number is also a power of 2. Note that, if there are initial zeros formed after the removal of the leading digit, then we also remove the initial zeros to get the new number.

10. The side lengths of a triangle are $2n-1$, $2n$ and $2n+1$, where n is a positive integer. If the triangle has an integer valued area less than 20000, find all possible areas of the triangle, and for each area, find the corresponding side lengths.

11. Show that
$$\frac{x^2-2}{2y^2+3}$$
is never an integer when x and y are integers.

12. Does there exist a set S of 21 consecutive positive integers such that, for each $x \in S$, x is divisible by some prime p from the interval $2 \leq p \leq 13$ (note that two distinct members of S can use two different primes from the interval)?

13. A circular table of radius r is pushed into a corner of a square room. A point on the edge of the table is at distance m from one wall, and n the other, where $m, n \leq r$. Suppose that m, n, r are integers, with m and n coprime. Prove that one of m and n is a perfect square, with the other even.

14. Can we find five distinct positive integers such that the sum of any three of them is prime?

15. Let $p > 0$ be prime. Prove that

    (a) $\binom{2p}{p} \equiv 2 \pmod{p^2}$,

    (b) $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for $0 \leq k \leq p-1$,

    where $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ denotes the binomial coefficient.

16. Prove that $\text{hcf}(a^m-1, a^n-1) = a^{\text{hcf}(m,n)}-1$ for every $a, m, n \in \mathbb{N}$, with $a \geq 2$.

17. For $n \in \mathbb{N}$, define $n!! = 1 \cdot 3 \cdot 5 \cdots n$ if n is odd, and $n!! = 2 \cdot 4 \cdot 6 \cdots n$ if n is even. Prove that $2005!! + 2006!!$ is divisible by 2007.

18. Let a and b be positive integers such that a^2+b^2 is divisible by ab. Prove that $a = b$.

19. Show that there are no integers x, y such that $x^3 - y^4 = 6$.

20. Prove that if m, n, r are positive integers such that
$$1 + m + n\sqrt{3} = (2+\sqrt{3})^{2r-1},$$
then m is a perfect square.

21. Let a, b, c be positive integers such that a is odd, $\operatorname{hcf}(a, b, c) = 1$, and

$$\frac{2}{a} + \frac{1}{b} = \frac{1}{c}.$$

Prove that abc is a perfect square.

22. Find all integer solutions to $x^2 + y^2 + z^2 = x^2y^2$.