Divisibility for Part IA Discrete Mathematics

Note: This handout contains some basic exercises for divisibility and a reminder of the definitions of the *division algorithm*, *remainder* and *modulo*.

Some common identities

Identities are very useful for number theory problems. We will see below examples for proving divisibility and examples for proving when an expression gives prime numbers.

Exercise 1. Show that

$$a^2 - b^2 = (a - b) \cdot (a + b)$$

.

Exercise 2. Show that

$$a^3 - b^3 = (a - b) \cdot (a^2 + ab + b^2)$$

.

Exercise 3. Show that

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$$

.

Exercise 4. Show that

$$a^3 + b^3 = (a + b) \cdot (a^2 - ab + b^2)$$

.

Exercise 5. Show that

$$a^{2n+1} + b^{2n+1} = (a + b) \cdot (a^{2n} - a^{2n-1}b + \ldots + b^{2n})$$

.

Division theorem and algorithm

Define the division algorithm and give OCaml code.

Theorem 1. For every natural number m and positive natural number n, the evaluation of `divalg`(m, n) terminates, outputing a pair of natural numbers (q_0, r_0) such that $r_0 < n$ and $m = q_0 \cdot n + r_0$.

Theorem 2. Show that there are unique naturals r and q such that $m = n \cdot q + r$ and $0 \leq r < n$.

Combining the above two theorems state the division theorem.

Remainder properties

There are two points when looking at these basic properties. One it to see how to derive them and the other is to understand what they mean so that you can use them when needed.

Property 1. For natural numbers $r, m\ell$, $\text{rem}(r \cdot m + \ell, m) = \text{rem}(\ell, m)$.

*Proof.*By the division theorem for ℓ and m, we have

$$\ell = \text{quo}(\ell, m) \cdot m + \text{rem}(\ell, m).$$

By adding $r \cdot m$ on both sides, we have

$$r \cdot m + \ell = r \cdot m + \text{quo}(\ell, m) \cdot m + \text{rem}(\ell, m) = (r + \text{quo}(\ell, m)) \cdot m + \text{rem}(\ell, m).$$

Note that $0 \leq \text{rem}(\ell, m) < m$. Hence, by the uniqueness of the remainder $\text{rem}(r \cdot m + \ell, m) = \text{rem}(\ell, m)$. □

Property 2. For natural numbers $r, m\ell$, $\text{rem}(k + \ell, m) = \text{rem}(\text{rem}(k, m) + \ell, m)$.

Proof. By the division theorem, $k = \text{quo}(r, m) \cdot m + \text{rem}(r, m)$.

$$\text{rem}(k + \ell, m) = \text{rem}(\text{quo}(r, m) \cdot m + \text{rem}(r, m) + \ell, m).$$

By the previous property,

$$\text{rem}(\text{quo}(r, m) \cdot m + \text{rem}(r, m) + \ell, m) = \text{rem}(\text{rem}(r, m) + \ell, m).$$

□

Property 3. For natural numbers $r, m\ell$, $\text{rem}(k \cdot \ell, m) = \text{rem}(k \cdot \text{rem}(\ell, m), m)$.

Proof. By the division theorem, $\ell = \text{quo}(\ell, m) \cdot m + \text{rem}(\ell, m)$, so

$$\text{rem}(k \cdot \ell, m) = \text{rem}(k \cdot (\text{quo}(\ell, m) \cdot m + \text{rem}(\ell, m)), m) = \text{rem}(k\,\text{quo}(\ell, m) \cdot m + k \cdot \text{rem}(\ell, m), m).$$

Hence, by Property 1, we have

$$\text{rem}(k\,\text{quo}(\ell, m) \cdot m + k \cdot \text{rem}(\ell, m), m) = \text{rem}(k \cdot \text{rem}(\ell, m), m).$$

□

In a large class of problems we are required to prove that $n \mid f(k)$ for some values of k. One approach to these problems is as follows:

- The division theorem tells us that $k = \text{quo}(k, n) \cdot n + r$ where $0 \leq r < n$.
- By considering all possible values of r, i.e. $0, 1, 2, \ldots, n-1$, we expand $f(\text{quo}(k, n) \cdot n + r)$.
- Perform a series of calculations and simplifications that show that $f(k)$ is of the form $n \cdot (\ldots)$.

Example 1. Prove that for any natural k, $3 \mid (k^3 - k)$.

Proof. Consider $k = 3\ell + r$ and $f(k) = k^3 - k = k(k^2 - 1) = k(k-1)(k+1)$.

- For $r = 0$, $f(k) = \overline{(3\ell)}(3\ell - 1)(3\ell + 1) = 3 \cdot (\ell(3\ell - 1)(3\ell + 1))$.
- For $r = 1$, $f(k) = \overline{(3\ell + 1)}\overline{(3\ell)}(3\ell + 2) = 3 \cdot ((3\ell + 1)\ell(3\ell + 2))$.
- For $r = 2$, $f(k) = (3\ell + 2)\overline{(3\ell + 1)}\underline{(3\ell + 3)} = 3 \cdot ((3\ell + 2)(3\ell + 1)(\ell + 1))$.

□

Note: Below we will use another technique that avoids factorisation. This is also a direct application

of Fermat's Little Theorem.

Example 2. Prove that for any natural k, $6 \mid k^3 + 3k^2 - 4k$.

*Proof.*Consider $k = 6\ell + r$ and $f(k) = k(k^2 + 3k - 4) = k(k-1)(k+4)$.

- For $r = 0$, $f(k) = (6\ell)(6\ell - 1)(6\ell + 4) = 6 \cdot (\ell)(6\ell - 1)(6\ell + 4)$.
- For $r = 1$, $f(k) = (6\ell + 1)(6\ell)(6\ell + 5) = 6 \cdot (6\ell + 1)\ell(6\ell + 5)$.
- For $r = 2$, $f(k) = (6\ell + 2)(6\ell + 1)(6\ell + 6) = 6 \cdot (6\ell + 2)(6\ell + 1)(\ell + 1)$.
- For $r = 3$, $f(k) = (6\ell + 3)(6\ell + 2)(6\ell + 1) = 3 \cdot 2 \cdot (3\ell + 1)(2\ell + 1)(6\ell + 1)$.
- For $r = 4$, $f(k) = (6\ell + 4)(6\ell + 3)(6\ell + 2) = 3 \cdot 2 \cdot (3\ell + 2)(3\ell + 1)(6\ell + 2)$.
- For $r = 5$, $f(k) = (6\ell + 5)(6\ell + 4)(6\ell + 3) = 2 \cdot 3 \cdot (6\ell + 5)(3\ell + 2)(2\ell + 1)$.

(Using the fact that 2, 3 are co-prime): Note that since 2 and 3 are co-prime it suffices to check that $2 \mid f(k)$ and $3 \mid f(k)$. You can do this as an exercise.

□

In the following example we take a few shortcuts in the computation:

Example 3. Show that $5 \mid k^5 - k$.

*Proof.*We start by factorising $f(k) = k(k^4 - 1) = k(k^2 - 1)(k^2 + 1) = k(k-1)(k+1)(k^2 + 1)$. Then consider $k = 5\ell + r$.

- For $r = 0, 1, 4$ one of the first three terms respectively is divisible by 5.
- For $r = 2$, $k^2 + 1 = (5\ell + 2)^2 + 1 = 5\ell^2 + 2 \cdot 5\ell + 4 + 1 = 5 \cdot (\ell^2 + 2\ell + 1)$.
- For $r = 3$, $k^2 + 1 = (5\ell + 3)^2 + 1 = 5\ell^2 + 2 \cdot 5\ell + 9 + 1 = 5 \cdot (\ell^2 + 2\ell + 2)$.

□

Example 4. Find the possible values of k such that $3 \mid (2k + 1)$.

*Proof.*Consider $k = 3\ell + r$ where $0 \leq r < 3$ and $f(k) = 2k + 1$.

- For $r = 0$, $f(k) = 2 \cdot (3\ell + 0) + 1 = 3 \cdot (2\ell) + 1$. Hence, $3 \nmid f(k)$.
- For $r = 1$, $f(k) = 2 \cdot (3\ell + 1) + 1 = 3 \cdot (2\ell + 1)$. Hence $3 \mid f(k)$.
- For $r = 2$, $f(k) = 2 \cdot (2\ell + 2) + 1 = 3 \cdot (2\ell) + 5$. Hence $3 \nmid f(k)$.

So, only for integers of the form $3k + 1$, $3 \mid f(k)$. □

Example 5. Prove that if k is an odd integer then $12 \mid (3k^2 + 12k + 21)$.

*Proof.*Since k is odd, it can be written as $k = 2\ell + 1$ for some $\ell \in \mathbb{Z}$. So,

$$3k^2+12k+21 = 3(2k+1)^2+12(2k+1)+21 = 3(4k^2+4k+1)+12(2k+1)+21 = 12(k^2+3k+1)+24 = 12\cdot(\ldots).$$

□

Example 6. Show that the product of n consecutive naturals is divisible by n.

Proof. The reason why this holds is that within n consecutive multiples there is a multiple of n. But we need to formalise this. Let k be the first of these naturals, then the product of the n naturals is

$$P = k(k+1)\cdot\ldots(k+(n-2))\cdot(k+(n-1))$$

Assume $k = n\cdot k' + r$ for $0 \leq r < n$. If $r = 0$, then $n \mid k$, so $n \mid P$. Otherwise, $n > n - r > 0$, so $k + n - r = n\cdot k' + r + n - r = n(k'+1)$, so $n \mid (k + n - r)$ and hence $n \mid P$. □

Exercise 6. Prove that for every natural k, $A = (5k+2)(3k+7)$ is even.

Exercise 7. Find the values of $k \in \mathbb{Z}$ such that $6 \mid (k^3 + 5k)$.

Exercise 8. Define an $f(k)$ such that for every natural k, $10 \mid f(k)$.

Exercise 9. Find the values of k such that $5 \mid 6k + 3$.

Exercise 10. Find the remainder of $A = 999^9 + 99^{99} + 9^{999} + 1$ with 9.

Exercise 11. Find the remainder of $A = 12! + 50$ with 33.

In the supervision work, you proved that:

- the product of two even numbers is even
- the product of two odd numbers is odd
- the sum of two even numbers is even
- the sum of two odd numbers is odd

These are useful facts which you can you to deduce the parity of several expressions.

Example 7. Prove that $x = k^2 + k + 1$ is odd for all natural k.

*Proof.*Assume k is even. Then k^2 is even, k is even, so $k^2 + k$ is even and $k^2 + k + 1$ is odd.

Assume k is odd. Then k^2 is odd, k is odd, so k^2+k is even and k^2+k+1 is odd. □

A generalisation of this is to find the possible remainders for various integers. For example the square of a natural can take the form 4ℓ or $4\ell+2$. This means that the two other forms $4\ell+1$ and $4\ell+3$. Let's prove this. Consider the square of an odd number $k=2\ell+1$, then $k^2=(2\ell+1)^2=4\ell^2+4\ell+1=4\underbrace{(\ell^2+\ell)}_{k}+1$.

Consider the square of an even number $k=2\ell$, then $k^2=(2\ell)^2=4\underbrace{\ell^2}_{k}$.

Example 8. Let k be a natural, prove that $A=\sqrt{4k+2}$ is non-integer.

Proof.

$$A=\sqrt{4k+2}\Rightarrow A^2=4k+2$$

But we know that the square of a number is of the form $4\ell+1$ or 4ℓ (for $\ell\in\mathbb{N}$), so there cannot be such A and k. □

Exercise 12. Prove that for odd $a,b\in\mathbb{N}$, the natural a^2+b^2 cannot be the square of a number.

Exercise 13. Prove that $(3k+2)(x+5)$ is even for all natural k.

Example 9. Prove that the square of an odd number is of the form $8k+1$.

*Proof.*Consider $n=2\ell+1$. Then $n^2=(2\ell+1)^2=4\ell^2+4\ell+1=4\ell(\ell+1)+1$. Since ℓ and $\ell+1$ are consecutive, one of them is even, so $\ell(\ell+1)$ is even say $2\ell'$ for $\ell'\in\mathbb{N}$. Then, $n^2=4\cdot(2\ell')+1=8\ell'+1$. □

Example 10. Let k be an odd number, show that $32\mid(k^2+3)(k^2+7)$.

*Proof.*By the previous exercise, $k^2=8k'+1$ for some $k'\in\mathbb{N}$, so $(k^2+3)(k^2+7)=(8k'+1+3)(8k'+1+7)=(8k'+4)(8k'+8)=4(2k'+1)8(k'+1)=32\cdot(...)$. □

Exercise 14. Let k be an odd number, show that $16\mid k^4-1$.

Exercise 15. Let a and b be odd, then prove that $8\mid(a^2-b^2)$.

Exercise 16. Find the remainder of n^4-n^2-1 with 2.

Exercise 17. Let a,b be naturals and $a+3b+2000^{2021}$. Prove that $2\mid(a+b)$.

Exercise 18. (a) Show that for a odd, $16\mid a^4-1$.

(b) Let $a,b\in\mathbb{N}$ be such that $ab=2021^{2021}$, show that $16\mid(a^4+b^4-1)$.

Exercise 19. Prove that the equation $x^2-1999^{2001}x+2001^{2007}=0$ does not have any integer solutions.

Exercise 20. Prove that if a and b are odd naturals, then the equation $x^{20}+ax^{11}+b=0$ has no integer solutions.

Exercise 21. Show that for a,b,c naturals, the number $\frac{(a+b)(b+c)(c+a)}{2}$ is natural.

Div

Define $n \mid m$.

Properties

Show that $d \mid n$ and $n \mid m$ implies that $d \mid m$.

Show that $d \mid n$ and $d \mid n$ implies that $d \mid n + m$.

Show that $d \mid n$, then $d \mid n \cdot m$.

[Linearity] Show that if $d \mid n$ and $d \mid m$, then $d \mid an + am$.

Attention ! $m \mid k$ and $n \mid k$ does not imply that $mn \mid k$.
Attention ! $k \mid mn$ does not imply that $k \mid m$ or $k \mid n$.

Now let's see how to apply the linearity property in some examples.

Example 11. Let a, b be naturals such that $7 \mid (45 + a)$ and $7 \mid (3 - b)$. Prove that $7 \mid (a + b)$.

Proof. We want to combine $45 + a$ and $3 - b$ such that the term $a + b$ appears. We do this using subtraction:

$$7 \mid (45 + a) \text{ and } 7 \mid (3 - b) \Rightarrow 7 \mid (45 + a - (3 - b)) \Rightarrow 7 \mid (42 + a + b).$$

Since $7 \mid 42$, we get that $7 \mid (42 + a + b - 42)$, so $7 \mid (a + b)$.

□

Example 12. Let a, b be naturals such that $11 \mid (5a + 6b)$, prove that $11 \mid (6a + 5b)$.

Proof. Trivially, $11 \mid 11(a + b)$, so $11 \mid (11a + 11b - (5a + 6b))$ which gives $11 \mid (6a + 5b)$. □

Example 13. Let n, d be naturals such that $d \mid n^2 + n + 1$ and $d \mid n^2 - n + 1$. Show that $d \mid 2$.

Proof. By the linearity property of divisibility, by taking the sum

$$d \mid n^2 + n + 1 \text{ and } d \mid n^2 - n + 1 \Rightarrow d \mid (n^2 + n + 1 + (n^2 - n + 1)) \Rightarrow d \mid 2n^2 + 2$$

and by taking the difference,

$$d \mid n^2 + n + 1 \text{ and } d \mid n^2 - n + 1 \Rightarrow d \mid (n^2 + n + 1 - (n^2 - n + 1)) \Rightarrow d \mid 2n.$$

Hence, $d \mid 2n^2 + 2$ and $d \mid 2n$. So, $d \mid (2n^2 + 2 - n \cdot (2n)) \Rightarrow d \mid 2$. □

Note: By noticing that $n^2 + n + 1$ is odd this means that $d \mid 1$ (*Why?*).

Example 14. Let d, n be naturals, such that $d \mid n^3 + n + 1$ and $d \mid n^2 - n + 1$. Show that $d = 1$.

*Proof.*The first step is to combine n^3+n+1 and n^2-n+1 so that n^3 vanishes. So,

$$d \mid (n^3+n+1-n\cdot(n^2-n+1)n^2) \Rightarrow d \mid (n^2+1)$$

Now we return to the second given equation,

$$d \mid (n^2+1-(n^2-n+1)) \Rightarrow d \mid n$$

which implies $d \mid n^2$ and hence $d \mid (n^2-n+1+(n^2)+n) \Rightarrow d \mid 1$. Hence, $d=1$. □

Example 15. Find all naturals n such that $(n+2) \mid (n^2+4)$.

*Proof.*One way of doing this is, $n+2 \mid (n+2)^2 \Rightarrow n+2 \mid (n^2+4n+4)$. By linearity of div, $n+2 \mid (n^2+4n+4-(n^2+4)) \Rightarrow n+2 \mid 4n$. Now we need to get something with $4n$, so $n+2 \mid 4(n+2)$, so by linearity $n+2 \mid 8$. So we just need to try the different divisors of 8, i.e. $n+2=2$, $n+2=4$ and $n+2=8$. These give the solutions $n=0,2,6$. (Note that you have to verify that $n+2 \mid (n^2+4)$ *Why?*) □

Exercise 22. Show that for naturals d,n such that $d \mid (5n+3)$ and $d \mid (8n+5)$ show that $d=1$.

Exercise 23. Show that for naturals d,n such that $d \mid (4k+2)$ and $d \mid (k^2+k)$, show that $d=2$.

Exercise 24. Show that for naturals a,b,d such that $d \mid (5a+17b)$ and $d \mid (2a+7b)$, $d \mid a$ and $d \mid b$.

Exercise 25. Find the largest natural that divides both $a=n^2+n+2$ and $b=n^2-n+2$.

Mod

Create a section similar to div and rem, containing the definition and properties of mod.

Using $(a+b)^n \equiv a^n \pmod{b}$

We will use the following relations to prove the divisibility relation:

$$(a+b)^n \equiv a^n \pmod{b}$$

Let us return to the following example:

Example 16. Prove that for any natural k, $3 \mid (k^3 - k)$.

Proof. Consider $k = 3\ell + r$ and $f(k) = k^3 - k$. Instead of factorising $f(k)$, we can use the fact that $(3\ell + r)^3 - (3\ell - r) \equiv r^3 - r \pmod 3$. So, it suffices to check:

- For $r = 0$, $r^3 - r = 0$.
- For $r = 1$, $r^3 - r = 1 - 1 = 0$.
- For $r = 2$, $r^3 - r = 2^3 - 2 = 6 \equiv 0 \pmod 3$.

□

Note: Sometimes it is convenient to take $r = -1$ instead of $r = 2$, which is valid since $2 \equiv -2 \pmod 3$.

Example 17. Prove that any natural of the form $n^4 + 4$ is composite, for $n > 1$ and n not a multiple of 5.

Proof. Consider numbers of the form $5k + r$ for $0 < r < 5$. Then $(5k+r)^4 + 4 \equiv (5k)^4 + r^4 + 4 \equiv r^4 + 4 \pmod 5$. So it remains to find the possible values for r^4. For $r = 1, 2, 3, 4$, we get $r^4 = 1, 16, 81, 256$ which are equivalent to $1, 1, 1, 1$. Hence, adding 4 gives a multiple of 5. □

Example 18. Let $a = 5^{2021} + 9^{2021} - 2$, show that $4 \mid a$.

Proof. $5^{2021} = (4+1)^{2021} \equiv 1 \pmod 4$ and $9^{2021} = (8+1)^{2021} \equiv 1 \pmod 8 \Rightarrow 9^{2021} \equiv 1 \pmod 4$.

Combining these, $5^{2021} + 9^{2021} - 2 \equiv 1 + 1 - 2 \equiv 0 \pmod 4$. □

Exercise 26. Prove that $A = 30^{2003} + 61^{2004}$ is divisible by 31.

Exercise 27. Prove that for all naturals $n \geq 1$, $A = 2^n \cdot 5^n + 3032$ is divisible by 9.

Using the identities that you proved above, for natural n, we have

$$(a-b) \mid a^n - b^n$$

and for any odd natural n, we also have,

$$(a+b) \mid a^n + b^n$$

Example 19. Show that $17 \mid 3^{2n} + 2^{3n}$ for odd natural n.

Proof. $3^{2n} + 2^{3n} = 9^n + 8^n$. Hence, $17 = (9 + 8) \mid (9^n + 8^n)$. □

Example 20. Show that $24 \mid (7^{2n} - 5^{2n})$ for every natural n.

Proof. We know that $7^{2n} - 5^{2n} = 49^n - 25^n$. So, $24 = 49 - 25 \mid 49^n - 25^n$. □

More exercises

Example 21. Find all integers k such that $(k - 2) \mid 7$.

Proof. 7 has four integer divisors $-1, 1, -7, 7$. These give $k = -5$, $k = 1$, $k = 3$ and $k = 9$. □

Example 22. Find all integers x and y such that $x + y = xy$.

Proof. To begin with, notice that there should not be many solutions to this because the RHS will become much larger than the LHS (e.g. take $y = 2$, $x + 2 = 2x$). An idea is to factor out one of the two terms,

$$x + y = xy \Leftrightarrow y = x(y - 1).$$

Which means that $y - 1 \mid y$. Hence, $y - 1 \mid (y - 1 - y) \Rightarrow y - 1 \mid -1$, which gives $y - 1 = 1 \Rightarrow y = 2$ or $y - 1 = -1 \Rightarrow y = 0$. For $y = 2$, we get $x = 2$ and for $y = 0$ we get $x = 0$. □

Exercise 28. Find integers x and y, such that $12x + y(1 - 2x) = 1$.

Exercise 29. Prove that for integers x and y, $x^2 - 3y = 17$ has no solutions.

Exercise 30. Prove that for naturals a, b, c, the differences $a - b$, $b - c$ and $c - a$, divide $A = a^2(b - c) + b^2(c - a) + c^2(a - b)$.

Exercise 31. (a) Prove that $a^3+b^3+c^3=(a+b+c)(a^2+b^2+c^2-ab-bc-ca)+3abc$.

(b) Show that for a,b,c naturals, $6 \mid (a+b+c)$ implies $6 \mid (a^3+b^3+c^3)$.

Exercise 32. For what values of n is $\sum_{k=1}^{n} k!$ a square?

Divisibility with induction

Example 23. Show that for natural n, $7 \mid (2^{n+2}+3^{2n+1})$.

*Proof.***(Base case)** For $n=0$, $2^{n+2}+3^{2n+1}=4+3=7$.

(Induction step) Assume true for $n=k$, i.e. $7\ell = 2^{k+2}+3^{2k+1}$, we will show that it is true for $n=k+1$,

$$2^{(k+1)+2}+3^{2(k+1)+1}=2^{k+2}\cdot 2^1+3^{2k+1}\cdot 3^2=(7\ell-3^{2k+1})\cdot 2+(3^{2k+1})\cdot 9=7(2\ell)+7\cdot(3^{2k+1})=7\cdot(\ldots)$$

□

Exercise 33. (a) $7|(5^{2n}+3\times 2^{5n-2})$.

(b) $13|(3^{n+2}+4^{2n+1})$.

(c) $27|(5^{n+2}+2^{5n+1})$.

Divisibility criteria and problems with digits

Whenever we are given to do an operation with the digits of a number N, it is convenient to write $N=\overline{x_{k-1}x_{k-2}\ldots x_1x_0}$ where the number has k digits. This means that in base 10 (for $0\le x_i\le 9$),

$$N=\sum_{i=0}^{k-1} x_i\cdot 10^i.$$

Similarly in the binary base, for $0\le x_i\le 1$),

$$N=\sum_{i=0}^{k-1} x_i\cdot 2^i.$$

Example 24. The sum of a 2-digit number N is 12. If we swap the digits, then the result is smaller by 18. Find the number.
s

*Proof.*Let $N=\overline{x_1x_0}$. The sum of the digits being 12 means that $x_1+x_0=12$. The swapped number is $N'=\overline{x_0x_1}=10x_0+x_1$. Hence, there difference being 18 means that $N-N'=18 \Rightarrow 10x_1+x_0-(10x_0+x_1)=9(x_1-x_0)=18\Rightarrow x_1-x_0=2$. Hence, $x=7$ and $y=5$. So $N=75$. □

Example 25. Show that N is divisible by 9 iff the sum of digits of N in base 10 are divisible by 9.

Proof.

$$N = \sum_{i=0}^{k-1} x_i \cdot 10^i = \sum_{i=0}^{k-1} x_i \cdot (9+1)^i \equiv \sum_{i=0}^{k-1} x_i \cdot 1^i \equiv \sum_{i=0}^{k-1} x_i \pmod 9$$

Hence, $9 \mid N$ iff $N \equiv 0 \pmod 9$ iff $\sum_{i=0}^{k-1} x_i \pmod 9$. □

Example 26. Let x and y be naturals such that (i) $x + y = 514$ and (ii) y is obtained from x by deleting the last digit.

Proof.(Solution 1) Note that x has to be a two digit number otherwise the sum of x and y would be above 1000. So $x = \overline{x_2 x_1 x_0}$ and $y = \overline{x_2 x_1}$. Hence, $x + y = 100x_2 + 10x_1 + x_0 + 10x_2 + x_1 = 110x_2 + 11x_1 + x_0 = 514$. Note that if $x_2 = 5$, then $110x_2 > 514$. Also, if $x_2 = 3$, then $11x_1 + x_0 = 184$, but this is not possible even if $x_1 = x_0 = 9$. Hence, $x_2 = 4$ and $11x_1 + x_0 = 74$. Again, if $x_1 < 6$, then the sum will be too small or if $x_1 > 6$, then the sum will be too large. So $x_1 = 6$ and $x_0 = 8$. So the numbers are $x = 468$ and $y = 46$.

(Solution 2) An alternative approach is to write $x = 10y + d$ where d is the last digit. So, $10y + d + y = 11y + d = 514$. One solution is when $y = \text{quo}(514, 11) = 46$ and $d = \text{rem}(514, 11) = 8$. If we increasing y by 1 then the sum is too large, while if we decrease it by 1 it is too small. Hence, $x = 468$ and $y = 46$. □

Exercise 34. Show that N is divisible by 3 iff the sum of digits of N in base 10 are divisible by 9.

Exercise 35. The positive integer N is expressed in base 9 as $(a_n a_{n-1} \ldots a_0)_9$.

(a) Show that N is divisible by 3 if the least significant digit, a_0 , is divisible by 3.

(b) Show that N is divisible by 2 if the sum of its digits is even.

(c) Without using a conversion to base 10, determine whether or not $(464860583)_9$ is divisible by 12.

Exercise 36. *(Assumes knowledge of* gcd*)*

(a) By solving $10x \equiv 1 \pmod 7$, show that -2 is an inverse of 10 $\pmod 7$.

(b) Show that if $7 \nmid a$ then $7|x$ iff $7 \mid a \cdot x$.

(c) Show that the following divisibility criterion for x works for 7:

(i) Remove the last digit from x to get $x_{1:(n-1)}$.

(ii) Subtract twice the last digit from $x' = x_{1:(n-1)} - 2x_0$.

(iii) Repeat for x'.

(iv) $7 \mid x$ iff $7 \mid x'$.

(*d*) Determine whether 7 divides 259 and 2481.

Exercise 37. Find the digits x and y such that $A = \overline{476x212y}$ is a multiple of 45.

Exercise 38. Find the digit x such that $\overline{x98} + \overline{86x} + \overline{6x9} = 1678$.

Exercise 39. Find the digits x and y such that $\overline{abab} - \overline{baba} = 7272$.

Prime numbers basics

Give the definition of a prime number.

Example 27. Show that if p, $p+2$ and $p+4$ are primes then $p = 3$.

*Proof.*Assume $p = 3k$ for some $k \in \mathbb{N}$, then $3k$ is prime only if $k = 1$. This gives the triple $3, 5, 7$.

Assume $p = 3k + 1$ for some $k \in \mathbb{N}$, then the three primes are $3k + 1$, $3k + 3$ and $3k + 4$. So the second prime $3k + 3$ should be divisible by 3. Hence, it must be 3, but then $1, 3, 4$ are not primes, so p cannot have this form.

Assume $p = 3k + 2$ for some $k \in \mathbb{N}$, then the three primes are $3k + 2$, $3k + 4$ and $3k + 6$. Hence, the third prime is $3(k + 2)$, but this has two factors greater than 1 for any k, so it cannot be prime. Therefore, there is no prime of this form. □

(optional) Computing prime numbers (under construction!)

Show that a composite number has a prime factor smaller than $\sqrt{n}$.

Show how to compute the divisors of a number in $\sqrt{n}$ time.

Implementation challenge: Read about the sieve of Eratosthenes method to compute the prime numbers. (See the Christmas exercises).

Finding all primes of a particular form

One common task is to search for all primes of a particular form.

Example 28. Find all primes of the form $k^3 - 1$ for natural $k \geq 1$.

*Proof.*Here is another example, where factorisation comes useful.

$$k^3 - 1 = (k-1)(k^2 + k + 1)$$

In order for $k^3 - 1$ to be prime it should be not be expressible as the product of two naturals greater than one. So one of the factors $k - 1$ and $k^2 + k + 1$ has to be 1.

(Case 1): $k - 1 = 1$, so $k = 2$. This gives $k^3 - 1 = 7$, which is indeed prime.

(Case 2): $k^2 + k + 1 = 1 \Rightarrow k(k+1) = 0$, which does not have roots $k \geq 1$. □

Example 29. Find all primes of the form $k^2 - 3k + 4$ for $k \in \mathbb{Z}$.

*Proof.*Let's start with factorising this expression $f(k) = k^2 - 3k - 4 = (k+1)(k-4)$. Since we want $f(k)$ to be prime, one of the two terms has to be 1 or -1. We take the four possible cases:

- $k + 1 = 1$, gives $k = 0$, for which $f(k) = -4$ (not prime).
- $k + 1 = -1$, gives $k = -2$, for which $f(k) = 6$ (not prime).
- $k - 4 = 1$, gives $k = 5$, for which $f(k) = 6$ (not prime).
- $k - 4 = -1$, gives $k = 3$, for which $f(k) = 4$ (not prime).

□

Example 30. Find all values of natural k such that $k - 3, k - 2, k + 6$ are all prime.

*Proof.*Note that $k - 3$ and $k - 2$ are consecutive so one is even and the other is odd. The only even prime is 2, hence, $k = 5$ and the three primes are $2, 3, 11$. □

Exercise 40. Let p be a prime, find all naturals n such that $n^2 + n + p = 1982$.

Exercise 41. Find all primes p and q such that $a = p^{p+1} + q^{q+1}$ is also prime.

Open problems: There exist some very similar problems that are are still not solved. This shows that the area is not yet fully understood.

- *Twin primes conjecture:* Do there exist infinitely many primes of the form p and $p + 2$?

- *Cousin primes conjecture:* Do there exist infinitely many primes of the form p and $p+4$?
- *k-tuple conjecture:* Are there infinitely many triples of primes $(p, p+2, p+6)$? Are there infinitely many triples of primes $(p, p+4, p+6)$? (Recall that in the divisibility handout you proved that 3 divides one of $p, p+2, p+4$)

See also the Fundamental Theorem of Arithmetic handout.

Proving properties of prime numbers

Example 31. Let $p \neq 2, 5$ be a ptime, then $10 \mid p^2 - 1$ or $10 \mid p^2 + 1$.

*Proof.*One option is to take all possible remainders with division by 10. Note that because p is prime, the possible remainders r are just $1, 3, 7, 9$ (a remainder of $5, 0$ implies division by 5 and an even remainder implies division by 2). Hence,

- for $r = 1$, $p^2 - 1 \equiv 0 \pmod{10}$.
- for $r = 3$, $p^2 - 1 \equiv 8 \pmod{10}$ and $p^2 + 1 \equiv 0 \pmod{10}$.
- for $r = 7$, $p^2 - 1 \equiv 8 \pmod{10}$ and $p^2 + 1 \equiv 0 \pmod{10}$.
- for $r = 9$, $p^2 - 1 \equiv 0 \pmod{10}$.

Which verifies that for all cases $10 \mid p^2 - 1$ or $10 \mid p^2 + 1$. □

Past papers

COMPUTER SCIENCE TRIPOS Part IA – 2015 – Paper 2

8 Discrete Mathematics (MPF)

(*a*) Prove that, for all natural numbers n,

$$n^{13} \equiv n \pmod{1365}$$

You may use any standard results provided that you state them clearly. [5 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2014 – Paper 2

7 Discrete Mathematics (MPF)

(*a*) Let m be a fixed positive integer.

(*i*) For an integer c, let $K_c = \{\, k \in \mathbb{N} \mid k \equiv c \pmod{m} \,\}$.

Show that, for all $c \in \mathbb{Z}$, the set K_c is non-empty. [2 marks]

(*ii*) For an integer c, let κ_c be the least element of K_c.

Prove that for all $a, b \in \mathbb{Z}$, $a \equiv b \pmod{m}$ iff $\kappa_a = \kappa_b$. [4 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2007 – Paper 2

3 Discrete Mathematics I (MPF)

(*a*) Given $a, b \in \mathbb{N}$ with $a \geq b$ prove carefully that there are unique values $q, r \in \mathbb{N}$ such that $a = qb + r$ and $0 \leq r < b$. [6 marks]