GCD, linear diophantine equations, CRT for Part IA Discrete Mathematics

Note: This handout contains several exercises and past papers relevant to the *greatest common divisor (GCD)*, including *linear congruence equations*, *linear Diophantine equations* and more. The *Chinese remainder theorem (CRT)* is not taught in lectures, but appears regularly in some form in the exams. So, I would recommend you go over this topic (and the other grey areas) and attempt the relevant past papers. As always first attempt to solve your problem on your own and then consult the answer.

The material in this handout appears in multiple books and other resources, so you will find a more complete treatment there. For example Chapter 2 & 4.4 in "Elementary Number Theory" by D. M. Burton and Chapter 4.5.2 in "The art of computer programming (Volume II)" by D. Knuth.

Greatest Common Divisor

Definition 1. Define the set of divisors $\mathrm{D}(n)$ for a natural number n.

Definition 2. Define the set of common divisors $\mathrm{CD}(n, m)$ for natural numbers n and m.

Definition 3. Define the *greatest common divisor* $\gcd(n, m)$ for two positive natural numbers n and m.

Note: It is not immediately obvious that such a number indeed exists. You need the GCD algorithm for that.

Very Basic properties

Here we will prove some basic properties that motivate the GCD algorithm.

Property 1. For natural numbers n, m, $\mathrm{CD}(n, m) = \mathrm{CD}(m, n)$.

Property 2. For natural numbers n, m, $\mathrm{CD}(n, m \cdot n) = \mathrm{D}(n)$.

Property 3. Let m and m' be natural numbers and let n be a positive integer such that $m \equiv m' \pmod{n}$, then $\mathrm{CD}(m, n) = \mathrm{CD}(m', n)$. (Slide 183)

Property 4. For natural numbers n, m, $\mathrm{CD}(n, m) = \mathrm{CD}(n, \mathrm{rem}(m, n))$.

Property 5. For natural numbers n, m,

$$\mathrm{CD}(n,m) = \begin{cases} \mathrm{D}(n) & \text{if } n \mid m, \\ \mathrm{CD}(n, \mathrm{rem}(m,n)) & \text{otherwise.} \end{cases}$$

GCD algorithm

Write OCaml code for computing the gcd using Euclid's algorithm (from now on we will refer to the algorithm as `gcd0`). (Slide 189)

Note 1: Be careful in the ordering of arguments in the recursive call. If you place them in the wrong order, it will result in an infinite loop.

Note 2: This is not the only algorithm that computes the gcd. There is also a method using the Fundamental Theorem of Arithmetic (see that handout for more details). Also, one of the Christmas projects is to derive Steiner's algorithm for the gcd.

Reason that your implementation terminates. (Slide 194)

Reason that your implementation computes a number g such that $\mathrm{CD}(m,n) = \mathrm{D}(g)$ (and deduce that the gcd exists). (Slide 194)

Example 1. Evaluate $\gcd(72, 28)$ using the Euclidean algorithm.

Proof.

$$\begin{aligned}\gcd(72,28) &= \gcd(28, \mathrm{rem}(72,28)) = \gcd(28,16)\\ &= \gcd(16, \mathrm{rem}(28,16)) = \gcd(16,12)\\ &= \gcd(12, \mathrm{rem}(16,12)) = \gcd(12,4)\\ &= 4\end{aligned}$$

□

Example 2. Evaluate $\gcd(13, 8)$ using the Euclidean algorithm.

Proof.

$$\begin{aligned}\gcd(13,8) &= \gcd(8, \mathrm{rem}(13,8)) = \gcd(8,5)\\ &= \gcd(5, \mathrm{rem}(8,5)) = \gcd(5,3)\\ &= \gcd(3, \mathrm{rem}(5,3)) = \gcd(3,2)\\ &= \gcd(2, \mathrm{rem}(3,2)) = \gcd(2,1)\\ &= 1\end{aligned}$$

□

Example 3. Show that for positive integers m and n, we have $\gcd(m, m+n) \mid n$.

*Proof.*By the properties of the `gcd0` algorithm we know that $\gcd(m, m+n) = \gcd(m, m+n-m) = \gcd(m, n)$. Since $\gcd(m, n) \mid n$, it follows that $\gcd(m, m+n) \mid n$. □

Example 4. Show that for any $a \in \mathbb{N}$, $\gcd(2a+1, 9a+4) = 1$.

Proof.

$$\begin{aligned}\gcd(2a+1, 9a+4) &= \gcd(2a+1, 9a+4-4\cdot(2a+1)) \\ &= \gcd(2a+1, a) \\ &= \gcd(2a+1-2\cdot a, a) \\ &= \gcd(1, a) = 1\end{aligned}$$

□

Example 5. Show that for any $a \in \mathbb{N}$, $\gcd(5a+2, 7a+3) = 1$.

Proof.

$$\begin{aligned}\gcd(5a+2, 7a+3) &= \gcd(5a+2, 7a+3-(5a+2)) \\ &= \gcd(5a+2, 2a+1) \\ &= \gcd(5a+2-2\cdot(2a+1), 2a+1) \\ &= \gcd(a, 2a+1) \\ &= \gcd(a, 1) = 1\end{aligned}$$

□

Exercise 1. Show that for all positive integers a:

(a) $\gcd(3a+1, 13a+4) = 1$

(b) $\gcd(5a+2, 7a+3) = 1$

Exercise 2. For any odd positive integer a, $\gcd(18a+10, 3a+2) = 1$.

Exercise 3. Create an exercise of the above form.

(grey area) GCD efficiency

As computer scientists we are interested in how efficient the gcd algorithm is. For this analysis, we will count the number of steps, i.e. the number divisions made by the algorithm.

Theorem 1. The `gcd0`(n, m) algorithm takes $O(\log(m+n))$ steps to terminate.

*Proof.*We will prove that when `gcd0`(m, n) is called, after two steps, either the algorithm terminates or the sum $m+n$ is decreased by a factor 2/3. This will mean that the algorithm can run for at most $\log_{3/2}(m+n)$ steps (after this number the sum would have to be 1 or less, but this is not possible).

Assume that $m \geq n$. We will consider two cases:

If $m \geq 2n$, then after one iteration the new parameters are $m' = n$ and $n' = \text{rem}(m, n) < n$ (if the algorithm does not terminate). Hence, the new sum is $m' + n' \leq n + n = \frac{2}{3}(2n + n) = \frac{2}{3}(m + n)$ and we have proved the requirement.

Otherwise ($m < 2n$). Assume that the algorithm does not terminate within the next two iterations. Then in one iteration, the parameters will be $m' = n$, $n' = m - n$ (since $m > n$) and in the second iteration these will be $m'' = m - n$ and $n'' = \text{rem}(n, m - n) < m - n$. Hence, $m'' + n'' < (m - n) + (m - n) = 2m - 2n \leq 4n - 2n = 2n \leq \frac{2}{3}(m + n)$. □

Note: In O-notation the base of the logarithm does not affect the result.

See the Fibonacci question in the supervision work for a worst-case execution of the GCD algorithm.

(optional) Lamé's theorem

We will now look at a slightly stronger result for the execution time of the Euclidean gcd algorithm.

Lemma 1. For natural numbers $m > n \geq 1$, if `gcd0` performs $k \geq 1$ steps, then $m \geq F_{k+2}$ and $n \geq F_{k+1}$.

*Proof.*The proof is by induction over k. Consider $k = 1$. Since $n \geq 1 = F_1$ and $m > n$, it means that $m \geq 2 = F_2$.

For the inductive step assume that this is true for $k = \ell$, we will show that it is also true for $k = \ell + 1$. Consider m and n for which `gcd0`(m, n) takes k steps, then the the next iteration has parameters $m' = n$ and $n' = \text{rem}(m, n)$ and terminates in ℓ steps. By inductive hypothesis $m' > F_{\ell+2}$ and $n' > F_{\ell+1}$. So,

$$m' + n' = n + \text{rem}(m, n) = n + (m - \text{quo}(m, n) \cdot n) \leq m$$

since $m > n$ implies $\text{quo}(m, n) \geq 1$. Thus,

$$m \geq m' + n' > F_{\ell+2} + F_{\ell+1} = F_{\ell+3} = F_{(\ell+1)+2},$$

which proves that it also holds for $k = \ell + 1$. Hence, by the principle ... . □

This implies Lamé's Theorem.

Theorem 2. For any natural $k \geq 1$, if $a > b \geq 1$ and $b < F_{k+1}$, then `gcd0`(m, n) requires fewer than k steps.

Extended GCD

Show how the extended GCD algorithm computes $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Note that there are two ways to compute the coefficients x and y: (i) the forward and (ii) the backward method. We will show both ways here, and from then on we use only the forward method.

Example 6. Express $\gcd(72, 28)$ as an integer linear combination of 72 and 28.

*Proof.*We start with the forward computation. In each step, we keep a linear combination of the gcd arguments in terms of $n = 72$ and $m = 28$.

$$\left|\begin{array}{l|l|l} 72 = 28 \cdot 2 + 16 & 28 = 1 \cdot 28 & 16 = 72 - 2 \cdot 28 = 1 \cdot 72 + (-2) \cdot 28 \\ 28 = 16 \cdot 1 + 12 & 16 = 1 \cdot 72 + (-2) \cdot 28 & 12 = 28 - 16 = (-1) \cdot 72 + 3 \cdot 28 \\ 16 = 12 \cdot 1 + 4 & 12 = (-1) \cdot 72 + 3 \cdot 28 & 4 = 16 - 12 = 2 \cdot 72 + (-5) \cdot 28 \\ 12 = 4 \cdot 3 + 0 & 4 = 2 \cdot 72 + (-5) \cdot 28 & \end{array}\right|$$

which gives $4 = 2 \cdot 72 + (-5) \cdot 28$, i.e. $x = 2$ and $y = -5$.

Note 1: When doing this computation on paper you don't need the first column. It was added here for clarity.

Note 2: Throughout the execution you need to be methodological and keep the same order in products involving the quotients.

Similarly, we can obtain the result with the backward algorithm. Note that you should follow the second column from bottom to top each time replacing the remainder by a linear coefficient of the divident and the quotient.

$$\left|\begin{array}{l|l} 72 = 28 \cdot 2 + 16 & 4 = 2 \cdot 16 + (-1) \cdot 28 = 2 \cdot (72 - 2 \cdot 28) + (-1) \cdot 28 = 2 \cdot 72 + (-5) \cdot 28 \\ 28 = 16 \cdot 1 + 12 & 4 = 1 \cdot 16 + (-1) \cdot 12 = 16 - (1 \cdot 28 - 1 \cdot 16) = 2 \cdot 16 + (-1) \cdot 28 \\ 16 = 12 \cdot 1 + 4 & 4 = 1 \cdot 16 + (-1) \cdot 12 \\ 12 = 4 \cdot 3 + 0 & \end{array}\right|$$

□

Example 7. Express $\gcd(54, 21)$ as an integer linear combination of 54 and 21.

*Proof.*Forward computation,

$$\left|\begin{array}{l} 54 = 21 \cdot 2 + 12 \\ 21 = 12 \cdot 1 + 9 \\ 12 = 9 \cdot 1 + 3 \\ 9 = 3 \cdot 3 + 0 \end{array}\right| \left|\begin{array}{l} 21 = 1 \cdot 21 \\ 12 = 54 + (-2) \cdot 21 \\ 9 = (-1) \cdot 54 + 3 \cdot 21 \\ 3 = 2 \cdot 54 + (-5) \cdot 21 \end{array}\right| \left|\begin{array}{l} 12 = 54 - 21 \cdot 2 = 54 + (-2) \cdot 21 \\ 9 = 21 - 12 = (-1) \cdot 54 + 3 \cdot 21 \\ 3 = 12 - 9 = 2 \cdot 54 + (-5) \cdot 21 \end{array}\right|$$

Backward computation,

$$\left|\begin{array}{l} 54 = 21 \cdot 2 + 12 \\ 21 = 12 \cdot 1 + 9 \\ 12 = 9 \cdot 1 + 3 \\ 9 = 3 \cdot 3 + 0 \end{array}\right| \left|\begin{array}{l} 3 = 2 \cdot (54 + (-2) \cdot 21) + (-1) \cdot 21 = 2 \cdot 54 + (-5) \cdot 21 \\ 3 = 12 - (21 - 12) = 2 \cdot 12 + (-1) \cdot 21 \\ 3 = 12 - 9 \end{array}\right|$$

□

Basic 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.

Notice that there will be using three types of arguments:

(a) to prove that g is the $\gcd(n, m)$ we show that for every d, $d \mid m$ and $d \mid n$ implies $d \mid g$.

(b) $\gcd(n, m) = 1$ iff there exist x, y such that $nx + my = 1$.

(c) we prove a property using the steps of the GCD algorithm.

Property 6. For any positive integer n, $\gcd(n, 1) = 1$.

Proof.(Using method (a)) OK we will do the first quite rigorously (but you don't have to use so much detail). We need to show that

$$1 \mid n \wedge 1 \mid 1 \wedge \forall d \in \mathbb{N}.d \mid 1 \wedge d \mid n \Rightarrow d \mid 1$$

$1 \mid n$ and $1 \mid 1$ follow trivially from the properties of divisibility.

For the quantification. Let d be arbitrary. Assume $d \mid n$ and $d \mid 1$, then $d \mid 1$ (trivially). Hence,

$$\forall d \in \mathbb{N}.d \mid 1 \wedge d \mid n \Rightarrow d \mid 1$$

Combining the three terms in conjunction we get the result. So, $\gcd(n, 1) = 1$.

(Using method (b)) By choosing $x = 1$ and $y = -(n - 1)$ we have that $1 \cdot n + (-(n - 1)) \cdot 1 = 1$

(Using method (c)) The `gcd0` algorithm terminates in the first step since $1 \mid n$, so 1 is the the gcd of the two numbers. □

Property 7. For any positive integer n, $\gcd(n, n) = n$. *(You can also prove using all three methods.)*

Property 8. For any positive integer n and m, $\gcd(n, m) = \gcd(m, n)$.

Proof.(Using method (a)) Let d be arbitrary. Then

$$\begin{aligned} d \mid \gcd(n, m) &\Leftrightarrow d \mid n \wedge d \mid m \\ &\Leftrightarrow d \mid m \wedge d \mid n \\ &\Leftrightarrow d \mid \gcd(m, n) \end{aligned}$$

Two numbers with the same set of divisors are equal, hence $\gcd(m, n) = \gcd(n, m)$. □

Property 9. For any positive integers n, m, ℓ, $\gcd(\ell, \gcd(m, n)) = \gcd(\gcd(\ell, m), n)$.

Proof.(Using method (a)) Let d be arbitrary. Then

$$\begin{aligned} d \mid \gcd(\ell, \gcd(m, n)) &\Leftrightarrow d \mid \ell \wedge d \mid \gcd(m, n) \\ &\Leftrightarrow d \mid \ell \wedge (d \mid m \wedge d \mid n) \\ &\Leftrightarrow (d \mid \ell \wedge d \mid m) \wedge d \mid n \\ &\Leftrightarrow d \mid \gcd(\ell, m) \wedge d \mid n \\ &\Leftrightarrow d \mid \gcd(\gcd(\ell, m), n) \end{aligned}$$

Hence, $\gcd(\ell, \gcd(m, n)) = \gcd(\gcd(\ell, m), n)$. □

Property 10 (Linearity)**.** For any positive integers n, m, ℓ, $\gcd(\ell \cdot n, \ell \cdot m) = \ell \cdot \gcd(n, m)$.

Proof.(Using methods (a) and (b)) We will prove that $\ell{\cdot}\gcd(n,m) \mid \gcd(\ell{\cdot}n, \ell{\cdot}m)$ and $\gcd(\ell{\cdot}n, \ell{\cdot}m) \mid \ell{\cdot}\gcd(n,m)$, hence they must be equal.

For the first part, there exist $x, y \in \mathbb{Z}$ such that $(\ell m)x + (\ell n)y = \gcd(\ell \cdot n, \ell \cdot m)$. By writing $m = m' \gcd(n,m)$ and $n = n' \gcd(n,m)$ we get

$(\ell \gcd(n,m))m'x + (\ell \gcd(n,m))n'y = \ell \gcd(n,m)(m'x + n'y) = \gcd(\ell \cdot n, \ell \cdot m) \Rightarrow \ell \gcd(n,m) \mid \gcd(\ell \cdot n, \ell \cdot m)$

For the second part, we use what we proved that there exists $k \in \mathbb{Z}$ such that $\ell k = \gcd(\ell n, \ell m)$. By the definition of the gcd, we have $\ell \cdot k \mid \ell m$ and $\ell \cdot k \mid \ell n$. By the properties of $\mid$, these in turn imply that $k \mid m$ and $k \mid n$. Hence, $k \mid \gcd(m,n)$ so $\ell k \mid \ell \gcd(m,n)$, i.e. $\gcd(\ell \cdot n, \ell \cdot m) \mid \ell \gcd(m,n)$.

(Using method (c)) See slides 205-207 in the lecture notes. □

Let's see some applications of these properties.

Example 8. Show that $\gcd(m,n) = m$ iff $m \mid n$.

Proof.($\Rightarrow$) Assume $m = \gcd(n,m)$, then $m \mid n$ by the property of the gcd.

($\Leftarrow$) $\gcd(m,n) = \gcd(m, k \cdot m) = m \cdot \gcd(1,k) = m$ where we used the linearity property of the gcd. *Can you see how you would use method (b)?* □

Example 9. Show that $k \mid mn$ and $\gcd(k,m) = 1$ implies $k \mid n$.

Proof.(Using properties of gcd) $k \mid mn$ implies that $mn = k \cdot \ell$ for $\ell \in \mathbb{Z}$.

$$\begin{aligned} n &= \gcd(k,m) \cdot n \ (\gcd(k,m) = 1) \\ &= \gcd(k \cdot n, m \cdot n) \ (\text{by linearlity on } n) \\ &= \gcd(k \cdot n, k \cdot \ell) \\ &= k \cdot \gcd(n, \ell) \ (\text{by linearity on } k) \end{aligned}$$

Hence, $k \mid n$.

(Using method (b)) Since $\gcd(k, m) = 1$, there exist $x, y \in \mathbb{Z}$ such that $kx + my = 1$. By multiplying both sides by n, we get $knx + mny = n \Rightarrow knx + k\ell y = n \Rightarrow k(nx + \ell y) = n \Rightarrow k \mid n$. □

Example 10. Show that for all positive integers a, b, c, if $\gcd(a, b) = 1$ then $\gcd(a \cdot b, c) = \gcd(b, c)$.

Proof.(Using properties of gcd)

$$\begin{aligned}
\gcd(b, c) &= \gcd(b \cdot \gcd(a, c), c) \\
&= \gcd(\gcd(ba, bc), c) \text{ (by linearity of gcd)} \\
&= \gcd(ba, \gcd(bc, c)) \text{ (by associativity of gcd)} \\
&= \gcd(ab, c \cdot \gcd(b, 1)) \text{ (by linearity of gcd)} \\
&= \gcd(ab, c)
\end{aligned}$$

Why did we multiply by $\gcd(a, c) = 1$*? This was a trick. We want to somehow create the term* ab*. This multiplication by* $1 = \gcd(a, c)$ *and then linearity allow us to do this. Some of the following examples and exercises use it.*

(Using method (a) and Euclid's Theorem) We know that $\gcd(b, c) \mid c$ and $\gcd(b, c) \mid b$, so $\gcd(b, c) \mid ab$. So $\gcd(b, c) \mid \gcd(ab, c)$.

We know that $\gcd(ab, c) \mid ab$ and $\gcd(ab, c) \mid c$, so $\gcd(\gcd(ab, c), a) \mid \gcd(ab, c)$ (and so $\gcd(\gcd(ab, c), a) \mid c$) and $\gcd(\gcd(ab, c), a) \mid c$ so $\gcd(\gcd(ab, c), a) \mid \gcd(a, c) = 1$. Hence, $\gcd(\gcd(ab, c), a) = 1$. By Euclid's Theorem, $\gcd(ab, c) \mid b$ and hence $\gcd(ab, c) \mid \gcd(b, c)$. □

Example 11. For any positive integers a, b, c, if $a \mid bc$ then $a \mid \gcd(a, b) \cdot \gcd(a, c)$.

Proof.$\gcd(a, b)\gcd(a, c) = \gcd(a\gcd(a, c), b\gcd(a, c)) = \gcd(a\gcd(a, c), \gcd(ab, bc)) = \gcd(a\gcd(a, c), \gcd(ab, ak)) =$ $\gcd(a\gcd(a, c), a\gcd(b, k)) = a \cdot \gcd(\gcd(a, c), \gcd(b, k))$ □

Example 12. For any positive integers a, b, c, if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Proof. $\gcd(a,c) = \gcd(a,\gcd(a,b)c) = \gcd(a,\gcd(ac,bc)) = \gcd(\gcd(a,ac),bc) = \gcd(a\cdot\gcd(1,c),bc) = \gcd(a,bc)$. □

Example 13. For any positive integers a,b,c, if $\gcd(a,b)=1$, $c \mid a$ then $\gcd(b,c)=1$.

Proof. $a = c\cdot k$ for $k\in\mathbb{Z}$. We know that $\gcd(b,c) \mid b$ and $\gcd(b,c) \mid c$, so $\gcd(b,c) \mid ck$. Hence, $\gcd(b,c) \mid \gcd(ck,b)$. □

Exercise 4. For any positive integers a,b,c,d if $\gcd(a,b)=1$ and $d \mid ac$ and $d \mid bc$ then $d \mid c$.

Exercise 5. For any positive integers a,b,c, if $\gcd(a,b)=1$ and $c \mid a+b$, then $\gcd(a,c)=\gcd(b,c)=1$.

Exercise 6. If $\gcd(a,b)=1$, then $\gcd(a^2,b)=1$ and $\gcd(a^2,b^2)=1$.

Exercise 7. If $\gcd(a,b)=1$, then $\gcd(a^k,b^k)=1$. (Use the previous exercise)

Applications

Euclid's Theorem

The following theorems are two theorems that are very useful in number theory. These are so fundamental that you may think that you don't even need to prove them.

Theorem 3 (Euclid's theorem)**.** For positive integers k,m and n, if $k \mid (mn)$ and $\gcd(k,m)=1$, then $k \mid n$.

Proof. Assume $k \mid (mn)$ and $\gcd(k,m)=1$. By definition of divisibility, $mn = k\cdot k'$. By Euclid's extended gcd algorithm, there exist $x,y\in\mathbb{Z}$, such that $kx+my=1$. By multiplying both sides by n we have

$$k(nx)+mnx = n \Rightarrow k(nx)+kk'y = n \Rightarrow k(nx+k'y) = n \Rightarrow k \mid n.$$

□

Theorem 4. For positive integers m, n and prime p, if $p \mid (mn)$, then $p \mid m$ or $p \mid n$.

*Proof.*Assume $p \mid (mn)$. Assume $p \nmid m$, then since $\gcd(p, m) \mid p$ $\gcd(p, m) = 1$ (as it cannot be p). Hence by Euclid's Theorem, $p \mid n$. Hence, one of the two must hold. □

Existence of a multiplicative inverse

Definition 4. The multiplicative inverse of a in $\mathbb{Z}_b$ is the element c such that $ac \equiv 1 \pmod{b}$. We denote this element c by a^{-1}.

Let's take a look at the inverses of the elements in $\mathbb{Z}_{10}$:

0	1	2	3	4	5	6	7	8	9
–	1	–	7	–	–	–	3	–	9

Note that all odd elements except 5 have an inverse and this inverse is unique. Since $5 \mid 10$, this is suspicious. Let's look at the inverses of elements of $\mathbb{Z}_{20}$:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
–	1	–	7	–	–	–	3	–	9	–	11	–	17	–	–	–	13	–	19

OK, this strengthens our observation that elements that do not share a factor with $b = 20$ (i.e. are co-prime with 20) have an inverse (and only those). We also note that inverses appear in pairs. Below we will formally prove these statements and show how to use the extended GCD algorithm to calculate the inverse.

Theorem 5. Element $a \in \mathbb{Z}_b$ has a multiplicative inverse in $\mathbb{Z}_b$ iff $\gcd(a, b) = 1$.

Proof.($\Rightarrow$) Assume that a has a multiplicative inverse, then $aa^{-1} \equiv 1 \pmod{b}$, i.e. there exists $k \in \mathbb{Z}$ such that $aa^{-1} + bk = 1$. The $\gcd(a, b)$ divides all linear combinations of a and b, hence $\gcd(a, b) | aa^{-1} + bk \Rightarrow \gcd(a, b) \mid 1$. Therefore, $\gcd(a, b) = 1$.

($\Leftarrow$) By the extended Euclid's algorithm we know that $\gcd(a, b) = 1$ implies that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Therefore, $ax = 1 - by$, so $ax \equiv 1 - by \equiv 1 \pmod{b}$. Hence, $[x]_b$ is a multiplicative inverse. (we need $[\cdot]_b$ to guarantee that the element is in $\mathbb{Z}_b = \{0, 1, \ldots, b-1\}$ □

Note that the ($\Leftarrow$) direction also gives a method for computing a^{-1}. Before looking into this let's verify that the inverse is unique. This also implies that the inverses appear in pairs.

Theorem 6. The inverse of an element $a \in \mathbb{Z}_b$ is unique.

*Proof.*Assume that c and c' are both inverses of a. Then by definition of an inverse, $ca \equiv 1 \pmod{b}(1)$ and $c'a \equiv 1 \pmod{b}$. By properties of mod we multiply by c' both sides of the first relation to get $(ca)c' \equiv c' \equiv \pmod{b}$.
By associativity of multiplication, we get $c(ac') \equiv c' \equiv \pmod{b}$. (this could be skipped)
Finally, using (2) we get $c1 \equiv c' \equiv \pmod{b}$. So, $c \equiv c' \equiv \pmod{b}$. □

Example 14. Find the multiplicative inverse of 17 in $\mathbb{Z}_{20}$.

Proof.(**Using extended GCD)**)

$20 = 17 \cdot 1 + 3$	$17 = (1) \cdot 17$	$3 = 20 - 17 = (1) \cdot 20 + (-1) \cdot 17$
$17 = 5 \cdot 3 + 2$	$3 = (1) \cdot 20 + (-1) \cdot 17$	$2 = 17 - 5 \cdot 3 = (-5) \cdot 20 + (6) \cdot 17$
$3 = 2 \cdot 1 + 1$	$2 = (-5) \cdot 20 + (6) \cdot 17$	$1 = 3 - 2 = (6) \cdot 20 + (-7) \cdot 17$
$2 = 2 \cdot 1 + 0$	$1 = (6) \cdot 20 + (-7) \cdot 17$	

Hence, $1 = (6) \cdot 20 + (-7) \cdot 17$. Therefore, the multiplicative inverse is $[-7]_{17} = 13$.

(**Using trial and error**) Since we have proved that every element that is co-prime to 20 has a unique inverse, if we find an element x that satisfies $17x \equiv 1 \pmod{20}$, then we are done (since $\gcd(17, 20) = 1$). After trying some of the other odd elements we see that $x = 13$ has $17 \cdot 13 = 221$ which has a remainder of 1 when divided with 20. □

Note: The second method is mostly useful when b is small.

Example 15. Find the multiplicative inverse of 13 in $\mathbb{Z}_{20}$.

Proof.(**Using extended GCD)**)

$$\left|\begin{array}{l|l|l} 20 = 11 \cdot 1 + 9 & 11 = 1 \cdot 11 & 9 = 20 - 11 = 1 \cdot 20 + (-1) \cdot 11 \\ 11 = 9 \cdot 1 + 2 & 9 = 1 \cdot 20 + (-1) \cdot 11 & 2 = 11 - 9 = (-1) \cdot 20 + 2 \cdot 11 \\ 9 = 2 \cdot 4 + 1 & 2 = (-1) \cdot 20 + 2 \cdot 11 & 1 = 9 - 4 \cdot 2 = 5 \cdot 20 + (-9) \cdot 11 \\ 2 = 1 \cdot 2 + 0 & 1 = 5 \cdot 20 + (-9) \cdot 11 & \end{array}\right|$$

Hence, $1 = 5 \cdot 20 - 9 \cdot 11$. Therefore, the multiplicative inverse is $[-9]_{20} = 11$

(**Using trial and error**) Since we have proved that every element that is co-prime to 20 has a unique inverse, if we find an element x that satisfies $11x \equiv 1 \pmod{20}$, then we are done. After trying some of the other odd elements we see that $x = 11$ has $11 \cdot 11 = 121$ which has a remainder of 1 when divided with 20. □

Implementation challenge: Find the inverse of a in $\mathbb{Z}_b$ using the extended gcd algorithm.

Exercise 8. Find the inverses for the following elements:

(a) Find the inverse of 17 in $\mathbb{Z}_{26}$.

(b) Find the inverse of 8 in $\mathbb{Z}_{63}$.

(c) Find the inverse of 9 in $\mathbb{Z}_{11}$.

You can verify your answers (and generate more examples) by running the extended GCD algorithm or by using this tool.

Let's take a look at how we can evaluate the multiplicative inverse of a power of an element.

Theorem 7. Let a be an element in $\mathbb{Z}_b$ with multiplicative inverse a^{-1}. Show that for $k \in \mathbb{N} \setminus \{0\}$, the inverse of $a^k = \underbrace{a \cdot \ldots \cdot a}_{k \text{ times}}$ is $(a^{-1})^k$ in $\mathbb{Z}_b$.

Proof. $a^k \cdot (a^{-1})^k \equiv \underbrace{a \cdot \ldots \cdot a}_{k \text{ times}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ times}} \equiv \underbrace{(a \cdot a^{-1}) \cdot \ldots \cdot (a \cdot a^{-1})}_{k \text{ times}} \equiv \underbrace{1 \cdot \ldots \cdot 1}_{k \text{ times}} \equiv 1 \pmod{b}$. □

Solving linear congruences

Now, we will take a look at the related task of solving linear congruence equations. These are equations of the form $ax \equiv b \pmod{m}$, where $a, m \in \mathbb{N} \setminus \{0\}$ and $b \in \mathbb{Z}$. We begin with the case where $\gcd(a, m) = 1$.

Theorem 8. If $\gcd(a, m) = 1$, then all solutions to $ax \equiv b \pmod{m}$ are given by $x = a^{-1}b + km$ for every $k \in \mathbb{Z}$.

Proof. Since $\gcd(a, m) = 1$, there exists $a^{-1} \in \mathbb{Z}_m$ (by Theorem 5). Therefore,

$$ax \equiv b \pmod{m} \Rightarrow x \equiv a^{-1}b \pmod{m} \Rightarrow x = a^{-1}b + km \text{ for some } k \in \mathbb{Z}$$

We verify that all values of this form also satisfy the given equation

$$a(a^{-1}b + km) \equiv (aa^{-1})b + km \equiv b + 0 \equiv b \pmod{m}.$$

□

Example 16. Solve $13x \equiv 4 \pmod{20}$.

Proof. We know from the exercises in the previous section that the inverse of 13 in $\mathbb{Z}_{20}$ is 11. So the general solution is for any $k \in \mathbb{Z}$, such that $11 \cdot 4 + 20k = 44 + 20k$. □

Exercise 9. Solve the following modular equations:

(a) $17x \equiv 3 \pmod{26}$.

(b) $8x \equiv 5 \pmod{63}$.

(c) $9x \equiv 8 \pmod{11}$.

(Optional) What does this basically mean when m is a prime? It means that if we pick any non-zero element in $\mathbb{Z}_m$, we get that $f(x) = a \cdot_m x$ is an one-to-one function. Let's take a look at $m = 11$ for $a = 1$, a $= 2$, $a = 3$,

	1	2	3	4	5	6	7	8	9	10
$a = 1$	1	2	3	4	5	6	7	8	9	10
$a = 2$	2	4	6	8	10	1	3	5	7	9
$a = 3$	3	6	9	1	4	7	10	2	5	8

Note that each row generates a different permutation of the elements in $\mathbb{Z}_m \setminus \{0\}$. As you will see in the algorithms course, it is common to choose m prime and any non-zero a (and possibly some b) and use the function $ax + b$ as a hash function or a pseudo-random number generator or for encryption.

Now let us turn to the case where $\gcd(a, m)$ is not necessarily 1.

Theorem 9. The equation $ax \equiv b \pmod{m}$ is solvable iff $\gcd(a, m) \mid b$. In case there are solutions, these are given by the solutions of $\frac{a}{\gcd(a,m)} \cdot x \equiv \frac{b}{\gcd(a,m)} \pmod{\frac{m}{\gcd(a,m)}}$.

*Proof.*Let x be a solution to the equation $ax \equiv b \pmod{m}$. This implies that $m \mid ax - b$. Since $\gcd(a, m) \mid m$ and $\gcd(a, m) \mid a$, we get $\gcd(a, m) \mid ax - b$ and $\gcd(a, m) \mid ax$. So, $\gcd(a, m) \mid b$ (since if a number divides two numbers then it also divides their difference). So, if $\gcd(a, m) \nmid b$, then the equation has no solutions.

Otherwise, $a = a' \cdot \gcd(a, m)$, $m = m' \cdot \gcd(a, m)$ and $b = b' \cdot \gcd(a, m)$ for some $a', b', m' \in \mathbb{Z}$. Hence, $ax \equiv b \pmod{m}$ is equivalent to

$$\begin{aligned} ax - b = km &\Leftrightarrow (\exists k \in \mathbb{Z}. a' \gcd(a, m)x - b' \gcd(a, m) = km' \gcd(a, m)) \\ &\Leftrightarrow (\exists k \in \mathbb{Z}. a'x - b' = m'k) \\ &\Leftrightarrow a'x \equiv b' \pmod{m'}. \end{aligned}$$

Since $\gcd(a', m') = 1$ (why?), from Theorem 8, this is solvable and the solutions are given by $(a')^{-1}b + km$ for every $k \in \mathbb{Z}$. □

Example 17. Find all solutions to $12x \equiv 8 \pmod{20}$.

*Proof.*In this case $a = 12$, $m = 20$, so $\gcd(a, m) = \gcd(2^2 \cdot 3, 2^2 \cdot 5) = 2^2 = 4$. Since $4 \mid 8$, there exist solutions which are given by the solution of $\left(\frac{12}{4}\right) \cdot x \equiv \frac{8}{4} \pmod{\frac{20}{4}}$ or equivalently $3x \equiv 2 \pmod{5}$. By trial and error the solution to this is given by $4 + 5k$ for every $k \in \mathbb{Z}$. □

Example 18. Find all solutions to $12x \equiv 2 \pmod{20}$.

*Proof.*Assume there exists x that solves this equation, then

$$20 \mid 12x - 2 \Rightarrow 20 \mid 2(6x - 1) \Rightarrow 10 \mid 6x - 1 \Rightarrow 2 \mid 6x - 1 \Rightarrow 2 \mid 1,$$

which is not the case. Hence, there are no solutions. □

Exercise 10. Solve the following linear congruence equations:

(*a*) $85x \equiv 15 \pmod{80}$.

(*b*) $85x \equiv 43 \pmod{80}$.

(*c*) $54x \equiv 48 \pmod{66}$.

(*d*) $20x \equiv 60 \pmod{780}$.

Exercise 11. Show that the following linear congruences have no solutions (without using a calculator):

(*a*) $3x \equiv 16 \pmod{12937912894121}$.

(*b*) $16x \equiv 22 \pmod{12937912894112}$.

(*c*) $15x \equiv 12 \pmod{2374932874235}$.

Exercise 12. What happens if $a = 0$ in $ax \equiv b \pmod{m}$?

Solving linear Diophantine equations

Theorem 10. The equation $ax+by = d$ for given $a, b \in \mathbb{N}\setminus\{0\}$ and $d \in \mathbb{Z}$ has a solution iff $\gcd(a, b) \nmid d$.

*Proof.*Assume $x, y \in \mathbb{Z}$ are solutions to the equation, so $ax + by = d$. By definition of gcd, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so $\gcd(a, b) \mid ax + by$ so $\gcd(a, b) \mid d$. (Or if you can prove it from scratch: so there exist $a', b' \in \mathbb{Z}$ such that $a = a' \cdot \gcd(a, b)$, hence $d = a' \gcd(a, b)x + b' \gcd(a, b)y = \gcd(a, b)(a'x + b'y) \Rightarrow \gcd(a, b) \mid d$)

Assume $\gcd(a, b) \mid d$, so $d = d' \gcd(a, b)$ for $d' \in \mathbb{Z}$. The extended gcd algorithm implies that there exist x and y such that $ax + by = \gcd(a, b)$, hence $a(xd') + b(yd') = d' \gcd(a, b) = d$ (by multiplying by d'). So, xd' and yd' are solutions to the equations (NOT the only ones). □

Note: The proof also gives us a way to compute a solution to the linear Diophantine equation if there exists one.

Example 19. Find any solution to the equation $15x + 8y = 1$.

Proof..

$$\left|\begin{array}{l} 15 = 8 \cdot 1 + 7 \\ 8 = 7 \cdot 1 + 1 \\ 7 = 1 \cdot 7 + 0 \end{array}\right| \quad \left|\begin{array}{l} 8 = (1) \cdot 8 \\ 7 = (1) \cdot 15 + (-1) \cdot 8 \\ 1 = (-1) \cdot 15 + (2) \cdot 8 \end{array}\right| \quad \left|\begin{array}{l} 7 = 15 - 8 = (1) \cdot 15 + (-1) \cdot 8 \\ 1 = 8 - 7 = (-1) \cdot 15 + (2) \cdot 8 \end{array}\right|$$

So, $1 = (-1) \cdot 15 + (2) \cdot 8$, which means that $x = -1$ and $y = 2$ is a solution. □

Example 20. Find any solution to the equation $15x + 8y = 3$.

*Proof.*Given that $x = -1$ and $y = 2$ is a solution to $15x + 8y = 1$, by multiplying by 3 we get $x = -3$ and $y = 6$, which satisfies $15x + 8y = 3$. □

Example 21. Find any solution to the equation $75x + 20y = 55$.

Proof..

$$\left|\begin{array}{l} 75 = 20 \cdot 3 + 15 \\ 20 = 15 \cdot 1 + 5 \\ 15 = 5 \cdot 3 + 0 \end{array}\right| \quad \left|\begin{array}{l} 20 = (1) \cdot 20 \\ 15 = (1) \cdot 75 + (-3) \cdot 20 \\ 5 = 20 - 15 \cdot 1 = (-1) \cdot 75 + (4) \cdot 20 \end{array}\right| \quad \left|\begin{array}{l} 15 = 75 - 20 \cdot 3 = (1) \cdot 75 + (-3) \cdot 20 \\ 5 = 20 - 15 \cdot 1 = (-1) \cdot 75 + (4) \cdot 20 \end{array}\right|$$

So, $5 = 20 - 15 \cdot 1 = (-1) \cdot 75 + (4) \cdot 20$, which means that $x = -1$ and $y = 4$ is a solution to $75x + 20y = 5$, so by multiplying by 11 we obtain $x = -11$ and $y = 44$ as a solution. □

Example 22. Show that the equation $24x + 16y = 62$ has no solutions in $\mathbb{Z}$.

Proof.$\gcd(16, 24) = 4$, but $4 \nmid 62$, so the equation has no solution over $\mathbb{Z}$. □

Exercise 13. Find any solution to the following equations:

(a) $22x + 17y = 1$.

(b) $22x + 17y = 3$.

(c) $32x + 23y = 1$.

(*d*) $32x + 23y = 4$.

(*e*) $121x + 44y = 11$.

(*f*) $121x + 44y = 33$.

You can verify your solutions (and generate more practice questions) using this tool.

Exercise 14. Show that the following equations have no solutions:

(*a*) $22x + 16y = 5$.

(*b*) $21x + 14y = 6$.

Exercise 15. Show that the following equations have no solutions:

- $127983712x + 32498734234y = 222348093421$.
- $12381201x + 130482924y = 4$.

Theorem 11. Let $a, b \in \mathbb{N} \setminus \{0\}$ and $d \in \mathbb{N}$ such that $\gcd(a, b) \mid d$. All solutions to $ax + by = d$ for $x, y \in \mathbb{Z}$, are given by $x = x_0 + \frac{a}{\gcd(a,b)} \cdot k$ and $y = y_0 - \frac{b}{\gcd(a,b)} \cdot k$ for some $k \in \mathbb{Z}$, where (x_0, y_0) is any initial solution.

*Proof.*Let $x = x_0 + t_1$ and $y = y_0 + t_2$ be solutions for some $t_1, t_2 \in \mathbb{Z}$. We will now derive necessary conditions on t_1 and t_2, and then we will show that these are also sufficient. We start by writing out,

$$ax + by = d \Leftrightarrow a(x_0 + t_1) + b(y + t_2) = d \Leftrightarrow (ax_0 + by_0) + at_1 + bt_2 = d \Leftrightarrow at_1 + bt_2 = \Leftrightarrow at_1 = -bt_2$$

We can write $a = a' \cdot \gcd(a, b)$ and $b = b' \cdot \gcd(a, b)$ with $\gcd(a', b') = 1$. So, $at_1 = -bt_2 \Leftrightarrow a't_1 = b't_2$. By Euclid's corollary, since $\gcd(a', b') = 1$, $a' \mid t_2$ and $b' \mid t_1$. Hence, $t_1 = b' \cdot t_1'$ and $t_2 = a' \cdot t_2'$. So, $a't_1 = -b't_2 \Leftrightarrow a'b't_1' = -a'b't_2' \Leftrightarrow t_1' = -t_2'$. Hence, by introducing a new name for t_1', we get $t_1 = \frac{b}{\gcd(a,b)} \cdot k$ and $t_2 = \frac{a}{\gcd(a,b)} \cdot k$ for some $k \in \mathbb{Z}$, i.e. $x = x_0 + bk$ and $y = y_0 - ak$.

Finally, we verify that these are solutions to the original equation (i.e. the condition is sufficient), $a(x_0 + \frac{b}{\gcd(a,b)}k) + b(y_0 - \frac{a}{\gcd(a,b)}k) = ax_0 + by_0 + \frac{ab}{\gcd(a,b)}k - \frac{ab}{\gcd(a,b)}k = ax_0 + by_0 = d$. □

Example 23. Find all solutions to the equation $15x + 8y = 1$.

*Proof.*By the previous exercise we know that $x_0 = -1$ and $y_0 = 2$ is a solution. Hence, all solutions are given by $x = x_0 + 8k = -1 + 8k$ and $y = y_0 - 15k = 2 - 15k$ for some $k \in \mathbb{Z}$. □

Example 24. Find all solutions to the equation $15x + 8y = 3$.

*Proof.*We know that $x_0 = -3$ and $y_0 = 6$ is a solution. Hence, all solutions have the form $x = x_0 + 8k = -3 + 8k$ and $y = y_0 - 8k = 6 - 8k$. □

Example 25. Find all solutions to the equation $75x + 20y = 55$.

*Proof.*Since $x_0 = -11$ and $y_0 = 44$ is a solution for $75x + 20y = 55$, all solutions to the equation are given by $x = x_0 + \frac{20}{\gcd(75,20)}k = -11 + 4k$ and $y = y_0 - \frac{75}{\gcd(75,20)} = 44 - 15k$ for some $k \in \mathbb{Z}$. □

Exercise 16. Find all solutions to the following equations:

(a) $22x + 17y = 1$.

(b) $22x + 17y = 3$.

(c) $32x + 23y = 1$.

(d) $32x + 23y = 4$.

(e) $121x + 44y = 11$.

(f) $121x + 44y = 33$.

You can verify your solutions (and get more practice) using this tool.

Exercise 17. See 2006p2q4 for solving linear Diophantine equations with the additional constraint that x and y are non-negative.

Exercise 18 (Frobenius Problem)**.** In this exercise, we are trying to find for $a, b \in \mathbb{Z}^+$ with $\gcd(a, b)$, the largest $m \in \mathbb{Z}$ that is not representable by $ax + by = m$ for $x, y \in \mathbb{N}$ (i.e. $x \geq 0, y \geq 0$).

(a) (Optional) Watch this Numberphile video.

(b) Show that for a given m, there is always a unique solution (x_0, y_0) such that $0 \leq x_0 < b$.

(c) Show that the larger x is, the smaller y must be.

(d) Show that given $0 \leq x_0 < b$, the smallest integer not representable with solution x_0 is given when $y_0 = -1$.

(e) Show that the smallest m not representable is for $x_0 = b - 1$ and $y_0 = -1$ and find its value.

(f) Explain why all ms greater than this value are representable.

(grey area) Higher-order congruence equations

Can we solve higher-order linear congruence equations? For example, can we solve $x^2 - 5x + 6 \equiv 0 \pmod{10}$? Of course the brute force strategy of trying all possible modula still works. Consider in turn $0, 1, 2, \ldots, 9$ and the only values that satisfy this are $2, 3, 7$ and 8.

A more principled approach is to see that we need to prove that $x^2 - 5x + 6 = (x-2)(x-3)$ and $10 \mid (x-2)(x-3)$ iff $2 \mid (x-2)(x-3)$ and $5 \mid (x-2)(x-3)$. By Euclid's theorem, we know that

$$2 \mid (x-2)(x-3) \Leftrightarrow 2 \mid (x-2) \text{ or } 2 \mid (x-3) \Leftrightarrow x = 2k \text{ or } x = 2k+1 \text{ for some } k \in \mathbb{Z},$$

which holds for all x. So, it remains to investigate the other case,

$$5 \mid (x-2)(x-3) \Leftrightarrow 5 \mid (x-2) \text{ or } 5 \mid (x-3) \Leftrightarrow x = 5k+2 \text{ or } x = x = 5k+3 \text{ for } k \in \mathbb{Z}.$$

The solutions have the form $x = 5k + 2$ or $x = 5k + 3$ for some $k \in \mathbb{Z}$. (Note: that this is equivalent to the solutions having the form $x = 10k + 2$, $x = 10k + 7$, $x = 10k + 3$ or $x = 10k + 8$, which confirms the solutions we found above).

For the more general case we need the Chinese Remainder Theorem.

(grey area) Chinese Remainder Theorem

The Chinese Remainder theorem states that if m and n are co-prime, then there is a one-to-one mapping between the remainders with division by mn and the pairs of remainders with division by n and division by m. More concretely, consider $m = 5$ and $n = 4$, two co-prime numbers. There are $mn = 20$ possible remainders, which are shown below together with their remainders in the division with m and n respectively (for example 7 gives $(\text{rem}(7,5), \text{rem}(7,4)) = (2,3)$.

0	1	2	3	4	5	6	7	8	9
$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$	$(4,0)$	$(0,1)$	$(1,2)$	$(2,3)$	$(3,0)$	$(4,1)$

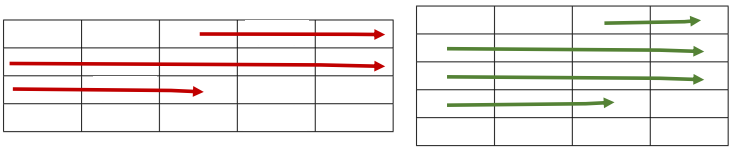
10	11	12	13	14	15	16	17	18	19
$(0,2)$	$(1,3)$	$(2,0)$	$(3,1)$	$(4,2)$	$(0,3)$	$(1,0)$	$(2,1)$	$(3,2)$	$(4,3)$

Note that none of the of the pairs appears in the output more than once. And also note that every pair appears once. To see why this holds it seems more natural to arrange the entries in a 4×5 and a 5×4 table, so that as we go through the entries in the table from left to right they yield the above sequence. This gives the following entries in the table

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$	$(4,0)$
$(0,1)$	$(1,2)$	$(2,3)$	$(3,0)$	$(4,1)$
$(0,2)$	$(1,3)$	$(2,0)$	$(3,1)$	$(4,2)$
$(0,3)$	$(1,0)$	$(2,1)$	$(3,2)$	$(4,3)$

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$
$(4,0)$	$(0,1)$	$(1,2)$	$(2,3)$
$(3,0)$	$(4,1)$	$(0,2)$	$(1,3)$
$(2,0)$	$(3,1)$	$(4,2)$	$(0,3)$
$(1,0)$	$(2,1)$	$(3,2)$	$(4,3)$

If two pairs are equal then they must be in the same column in the first and in the second array (why?). Now, look at the distance d between the two pairs (red and green arrow), which is the same on both arrays. Since the two elements are in the same column it must be that $m \mid d$ and similarly $n \mid d$. But the lowest common multiple $\text{lcm}(n, m) = \frac{mn}{\gcd(n,m)} = mn$ (see the Fundamental Theorem of Arithmetic handout), and $0 < d < mn$ (as the distance between two different elements in a collection of mn elements). Hence, there cannot exist such distance. Since there are mn elements that are different, it must be a one-to-one mapping.



Now, we will prove the existence part in a constructive way, i.e. one that allows to compute the value $x \in \mathbb{Z}_{mn}$ such that $\text{rem}(x, m) = x_1 \in \mathbb{Z}_m$ and $\text{rem}(x, n) = x_2 \in \mathbb{Z}_n$.

Theorem 12. Let $m, n \in \mathbb{N} \setminus \{0\}$ with $\gcd(n, m) = 1$, $x_1 \in \mathbb{Z}_m$ and $x_2 \in \mathbb{Z}_n$. Then, there exists unique $x \in \mathbb{Z}_{mn}$, such that $\text{rem}(x, m) = x_1$ and $\text{rem}(x, n) = x_2$.

*Proof.*Since m and n are co-prime, there exist $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Consider $x = [x_1 ny + x_2 mx]_{mn}$. *How did we choose this?* If look at the remainder of x divided by m, we have

$$x \equiv (x_1 ny + x_2 mx) \equiv x_1 ny \equiv x_1(1 - mx) \equiv x_1 \pmod{m}.$$

Similarly, $x \equiv x_2 \pmod{n}$. Hence, this weighing □

Note: In one of the Christmas projects, you are asked to prove that the Chinese remainder theorem generalises to more than one pairwise co-prime numbers.

Example 26. Find all $x \in \mathbb{Z}_{15}$ such that $\text{rem}(x, 5) = 3$ and $\text{rem}(x, 3) = 1$.

s

Proof.(**Brute force**) We know that there are just 15 numbers to check, so we go through all of them and see which one satisfies both. (Actually we only need to check numbers of the form $5k + 3$). In this way we find the answer 13.

(**Using gcd**) Note that $(-1) \cdot 5 + (2) \cdot 3 = 1$. Hence, $x = [1 \cdot (-1) \cdot 5 + 3 \cdot (2) \cdot 3]_{15} = 13$. □

Example 27. Find all $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{41}$ and $x \equiv 10 \pmod{47}$.

*Proof.*By the extended gcd algorithm we get $(-8) \cdot 41 + 7 \cdot 47 = 1$. Hence, the initial solution is given by $[10 \cdot (-8) \cdot 41 + 3 \cdot 7 \cdot 47]_{41 \cdot 47} = 1561$. Hence, the general solution is $x = 1561 + 41 \cdot 47k$ for some $k \in \mathbb{Z}$. □

Example 28. Find all $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{41}$ and $7x \equiv 23 \pmod{47}$.

*Proof.*First of all, we notice that $7x \equiv 10 \pmod{47}$ does not have the form we need for the CRT. But we know that 7 has a multiplicative inverse (which we find to be 27) in $\mathbb{Z}_4 7$, hence $7x \equiv 23 \pmod{47}$ is equivalent to $27 \cdot 7x \equiv 27 \cdot 23 \pmod{47}$ which is equivalent to $x \equiv 3 \pmod{47}$.

Hence, we now have to solve the system $x \equiv 3 \pmod{41}$ and $x \equiv 10 \pmod{47}$, which we did in the previous exercise. □

Exercise 19. Show that for $m = 4$ and $n = 2$, there exists a counterexample to the one-to-one mapping.

Examples

Example 29. (Requires knowledge of the Chinese Remainder Theorem) Find the last two digits of 3^{400}.

*Proof.*We want to determine the remainder of 3^{400} when divided by 100, i.e. by $5^2 \cdot 2^2$. Note that $\phi(25) = 20$ and $\phi(4) = 1$. By Euler-Fermat's theorem, $3^{20} \equiv 1 \mod 25$ so $3^{400} \equiv 1 \mod 25$ and $3^2 \equiv 1 \mod 4$ so $3^{400} \equiv 1 \mod 4$. Hence, using the Chinese Remainder Theorem since $\gcd(4, 100) = 1$, $3^{400} \equiv 1 \mod 100$ and so the last two digits are 01. □

Problems (under construction)

Past papers

COMPUTER SCIENCE TRIPOS Part IA – 2017 – Paper 2

7 Discrete Mathematics (MPF)

(*a*) (*i*) Calculate $\gcd(144, 77)$, the greatest common divisor of 144 and 77, as an integer linear combination of 144 and 77. [4 marks]

(*ii*) What is the multiplicative inverse of 77 in $\mathbb{Z}_{144}$ and the multiplicative inverse of 67 in $\mathbb{Z}_{77}$? [2 marks]

(*iii*) Describe all integers x that solve the following two congruences

$$\begin{cases} 77 \cdot x \equiv 1 \pmod{144} \\ 67 \cdot x \equiv 3 \pmod{77} \end{cases}$$

Indicate how one may calculate the least natural number solution to the above. [4 marks]

Justify your answers.

COMPUTER SCIENCE TRIPOS Part IA – 2017 – Paper 2

8 Discrete Mathematics (MPF)

(*a*) For a non-empty tuple of positive integers $a_1, \ldots, a_n$, let

$$\mathrm{CD}(a_1, ..., a_n) = \{\, d \in \mathbb{N} : \forall\, 1 \leq i \leq n.\ d \mid a_i \,\}$$

be the set of natural numbers that are common divisors of all $a_1, \ldots, a_n$.

(*i*) Without using the Fundamental Theorem of Arithmetic, prove that for positive integers a and a', if $\mathrm{CD}(a, a') = \{1\}$ then, for all integers k,

$$(a \cdot a') \mid k \iff a \mid k \wedge a' \mid k$$ [4 marks]

(*ii*) Either prove or disprove that, for all natural numbers $n \geq 2$ and all tuples of positive integers $a_1, \ldots, a_n$, if $\mathrm{CD}(a_1, \ldots, a_n) = \{1\}$ then, for all integers k, $(a_1 \cdot \ldots \cdot a_n) \mid k \implies a_1 \mid k \wedge \ldots \wedge a_n \mid k$. [3 marks]

(*iii*) Either prove or disprove that, for all natural numbers $n \geq 2$ and all tuples of positive integers $a_1, \ldots, a_n$, if $\mathrm{CD}(a_1, \ldots, a_n) = \{1\}$ then, for all integers k, $a_1 \mid k \wedge \ldots \wedge a_n \mid k \implies (a_1 \cdot \ldots \cdot a_n) \mid k$. [3 marks]

7 Discrete Mathematics (MPF)

You may use standard results provided that you mention them clearly.

(*a*) (*i*) State a sufficient condition on a pair of positive integers a and b so that the following holds:

$$\forall\, x, y \in \mathbb{Z}.\, \big(x \equiv y \pmod{a} \wedge x \equiv y \pmod{b}\big) \iff x \equiv y \pmod{ab}$$

[2 marks]

(*ii*) Recall that, for a positive integer m, we let $\mathbb{Z}_m = \{n \in \mathbb{N} \mid 0 \leq n < m\}$ and that, for an integer k, we write $[k]_m$ for the unique element of $\mathbb{Z}_m$ such that $k \equiv [k]_m \pmod{m}$.

Let a and b be positive integers and let k and l be integers such that $k\,a + l\,b = 1$. Consider the functions $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ and $g : \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{ab}$ given by

$$f(n) = \big([n]_a\,,\, [n]_b\big)\ , \quad g(x, y) = [k\,a\,(y - x) + x]_{ab}$$

Prove either that $g \circ f = \mathrm{id}_{\mathbb{Z}_{ab}}$ or that $f \circ g = \mathrm{id}_{\mathbb{Z}_a \times \mathbb{Z}_b}$. [8 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2016 – Paper 2

8 Discrete Mathematics (MPF)

(*a*) (*i*) Calculate two integers x and y satisfying $177\,x + 78\,y = 3$. [3 marks]

(*ii*) Describe all the integer pairs (x, y) that satisfy the above equation. [3 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2016 – Paper 2

9 Discrete Mathematics (MPF)

(*a*) Let p and m be positive integers such that $p > m$.

(*i*) Prove that $\gcd(p, m) = \gcd(p, p - m)$. [3 marks]

(*ii*) Without using the Fundamental Theorem of Arithmetic, prove that if $\gcd(p, m) = 1$ then $p \,|\, \binom{p}{m}$. You may use any other standard results provided that you state them clearly. [3 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2015 – Paper 2

7 Discrete Mathematics (MPF)

(*a*) Let $\mathbb{N}_{\geq 2} \stackrel{\text{def}}{=} \{\, k \in \mathbb{N} \mid k \geq 2 \,\}$.

Without using the Fundamental Theorem of Arithmetic, prove that for all positive integers m and n,

$$\gcd(m, n) = 1 \iff \neg(\, \exists\, k \in \mathbb{N}_{\geq 2}.\ k \,|\, m \wedge k \,|\, n \,)$$

You may use any other standard results provided that you state them clearly. [6 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2015 – Paper 2

9 Discrete Mathematics (MPF)

(*a*) Without using the Fundamental Theorem of Arithmetic, prove that for all positive integers a, b, c,

$$\gcd(a, c) = 1 \implies \big(\ \gcd(a \cdot b, c) \,|\, b \wedge \gcd(a \cdot b, c) = \gcd(b, c)\ \big)$$

You may use any other standard results provided that you state them clearly. [6 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2014 – Paper 2

7 Discrete Mathematics (MPF)

(*c*) (*i*) Use Euclid's Algorithm to express the number 1 as an integer linear combination of the numbers 34 and 21. [3 marks]

(*ii*) Find a solution $x \in \mathbb{N}$ to $34 \cdot x \equiv 3 \pmod{21}$. [3 marks]

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]

(*b*) Prove further that the greatest common divisor of a and b is equal to the greatest common divisor of b and r. [2 marks]

(*c*) Derive Euclid's algorithm for finding the greatest common divisor of two numbers. [3 marks]

(*d*) Determine the algorithm's efficiency by finding a limit for the number of divisions required in its execution expressed as a function of a. [3 marks]

(*e*) Find all values $x, y \in \mathbb{Z}$ satisfying $72x + 56y = 40$. [3 marks]

(*f*) Find all values $z \in \mathbb{Z}$ satisfying $56z \equiv 24 (\text{mod } 72)$. Express the answer in the form $z \equiv a (\text{mod } m)$. [3 marks]

COMPUTER SCIENCE TRIPOS Part IA – 2003 – Paper 1

2 Discrete Mathematics (MPF)

(*a*) Show that the greatest common divisor of 798 and 567 is 21. [2 marks]

(*b*) Find all pairs of integers (x, y) with $798x + 567y = 63$. [4 marks]

(c) Find all integer solutions to $567x = 42 \pmod{798}$. [4 marks]