GCD and φ

1 GCD

Definition 1 — Given two integers a and b, the *greatest common divisor* of them is the largest natural number that is a factor of both a and b, denoted $\gcd(a, b)$.

a and b are *relatively prime* if they share no common factors greater than 1 (in which case $\gcd(a, b) = 1$).

Example 1 — $\gcd(24, 36) = 12$, $\gcd(7, 9) = 1$, $\gcd(29305, 25) = 5$.

Note that $\gcd(n, 0) = n$ because $n \mid 0$ for any n.

One way to find the greatest common divisor of two numbers is by looking at their prime factorizations and, for each shared prime factor, finding the highest power of said prime that divides both numbers, and multiplying all these shared prime power factors together.

Example 2 — $74299680 = 2^5 \cdot 3^6 \cdot 5 \cdot 7^2 \cdot 13$, and $13640319000 = 2^3 \cdot 3^11 \cdot 5^3 \cdot 7 \cdot 11$, so we have

$$\gcd(74299680, 13640319000) = 2^3 \cdot 3^6 \cdot 5 \cdot 7 = 204120.$$

However, this method of finding the gcd requires having the prime factorization of a number, which may be time-consuming to find.

2 Euclidean Algorithm

Given two nonzero integers a and b, the *Euclidean algorithm* produces $\gcd(a, b)$ without needing to factor a or b into primes. Here's how it works.

Algorithm 1 (Euclidean Algorithm)

If $a = b$, we have $\gcd(a, b) = a$ and we are done. Otherwise, using division with remainder, we may write $a = qb + r$ for some r such that $0 \leq r < b$. If $r = 0$, then $b \mid a$ and $\gcd(a, b) = b$. If $r > 0$, we can *iterate*:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

until we reach a remainder of 0. If $r_{k+1} = 0$, say, then the last line of the computation will be

$$\vdots$$

$$r_{k-1} = q_{k+1} r_k.$$

We claim then that $\gcd(a, b) = r_k$.

Remark. Division with remainder is a much faster operation than finding the prime factorization–which requires a lot of *trial* division with remainder at our current stage.

Note that this algorithm *must* terminate since $r_1, r_2, \ldots$ form a decreasing sequence of natural numbers—so it must not have more than r_1 steps!

Why does this algorithm work? Let's see.

Lemma 1

If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Proof. We have $n \mid a - b$, so every divisor of n divides $a - b$.

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

Similarly, if $d \mid n$ and $d \mid b$, then $d \mid (b + (a - b)) = a$.

Thus we see that a and b have the same factors in common with n. Since the gcd is the *greatest* common factor, we conclude $\gcd(a, n) = \gcd(b, n)$. □

Theorem 2

In the algorithm above,

$$\gcd(a, b) = r_{k-1}.$$

(If $k = 1$, then $\gcd(a, b) = b$.)

Proof. Let $r_0 = b$ and $r_{-1} = a$, Then

$$r_{i-2} = q_i r_{i-1} + r_i$$

for all $1 \leq i \leq k$. That is,

$$r_{i-2} \equiv r_i \pmod{r_{i-1}}$$

for all i. By repeated application of the Lemma (and symmetry of the gcd function),

$$\gcd(a, b) = \gcd(r_{-1}, r_0)$$

$$
\begin{aligned}
&= \gcd(r_1, r_0) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_3, r_2) \\
&\vdots \\
&= \gcd(r_k, r_k + 1) = \gcd(r_k, 0) = |r_k| = r_k. \qquad \square
\end{aligned}
$$

Example 3 — Take $a = 78$ and $b = 33$. Then

$$
\begin{aligned}
78 &= 2 \cdot 33 + 12 \\
33 &= 2 \cdot 12 + 9 \\
12 &= 1 \cdot 9 + 3 \qquad \leftarrow \text{there's the gcd!} \\
9 &= 3 \cdot 3
\end{aligned}
$$

so $\gcd(78, 33) = 3$.

Exercise 1. Compute the gcd of 2024 and your student number.

Example 4 — (Note: Not an actual student number, hopefully.)

$$
\begin{aligned}
1021722031 &= 504803 \cdot 2024 + 759 \\
2024 &= 2 \cdot 759 + 506 \\
759 &= 1 \cdot 506 + 253 \\
506 &= 2 \cdot 253
\end{aligned}
$$

so $\gcd(1021722031, 2024) = 253$. Compare this with trying to factor both numbers first. Yeah, $2024 = 2^3 \cdot 11 \cdot 23$, but what about 1021722031?

3 Bézout's identity

A byproduct of the Euclidean algorithm is we've got all these equations relating the quotients and remainders. By re-writing each line as

$$r_i = r_{i-2} - q_i r_{i-1}$$

(except the last), we can work backwards and express $r_k = \gcd(a, b)$ as a linear combination of a and b.

Example 5 — From our previous computation of $\gcd(78, 33) = 3$,

$$\begin{aligned} 78 &= 2 \cdot 33 + 12 & & \\ 33 &= 2 \cdot 12 + 9 & & \\ 12 &= 1 \cdot 9 + 3 & 3 &= 12 - 1 \cdot 9 \\ & & 3 &= 12 - 1 \cdot (33 - 2 \cdot 12) = 3 \cdot 12 - 1 \cdot 33 \\ & & 3 &= 3 \cdot (78 - 2 \cdot 33) - 1 \cdot 33 = 3 \cdot 78 - 7 \cdot 33 \end{aligned}$$

i.e. we can write $3 \cdot 78 - 7 \cdot 33 = 3$.

In general, if $\gcd(a, b) = d$, then there exist integers s, t such that

$$as + bt = d.$$

This is known as *Bézout's identity*, and it's especially useful when a and b are coprime.

Theorem 3 (Bézout's identity)

Let a, b be nonzero integers. The equation $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

Proof. Denote $d = \gcd(a, b)$.

The only if direction is easy: since $d \mid a$ and $d \mid b$, we know $d \mid (as + bt)$ for any s, t, so $d \mid c$.

As for the if direction:

Consider the set S of natural numbers that can be expressed as an integer combination of a and b. That is, $S = \{an + bm : n, m \in \mathbb{Z}, an + bm \geq 1\}$.

Clearly, S is nonempty: Choose $n = 1$ for $a > 0$ and $n = -1$ for $a < 0$, same with m and b, then we get $an > 0$ and $bm > 0$, and so $an + bm > 0$. Then we may apply Well-Ordering Principle[*] to S and conclude that S has some least element $d = as + bt$. We claim that $d = \gcd(a, b)$.

We first show that d is a common factor of a and b. Write $a = dq + r$ with $0 \leq r < d$, then we have $a = (as + bt)q + r$ and so $r = a(1 - s) + b(-qt)$ can be expressed as a linear combination of a and b. However, d is the least element of S and $r < d$, so we must have $r = 0$ and hence $d \mid a$. Similarly, we can conclude that $d \mid b$.

Now for any common factor f of a and b, we have $f \mid (as + bt) = d$ and so $f \leq d$, so d is the *greatest* common divisor of a and b.

Returning to the if direction of our Theorem, if $c = qd$, we can take $x = qs$ and $y = qt$, then $aqs + bqt = qd = c$ and so $ax + by = c$ has integer solutions. $\square$

[*] That any nonempty subset of $\mathbb{N}$ has a least element.

Exercise 2. Use the above method to express 1 as an integer combination of 196 and 213.

Exercise 3. Find an integer combination of 2024 and your student number that equals their gcd.

4 Euler φ

Definition 2 — The *totient* of n is the number of integers between 1 and n that are coprime to n.

$$\varphi(n) = |\{1 \leq a \leq n : \gcd(a, n) = 1\}|$$

Exercise 4. Fill in the first dozen values of $\varphi(n)$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$												4

Proposition 4

Let p be a prime and let k be a positive integer. Then

$$\varphi(p^k) = p^{k-1}(p-1).$$

In particular, $\varphi(p) = p - 1$.

Proof. The numbers that are *not* coprime to p^k are necessarily multiples of p. Between 1 and p^k, the multiples of p are

$$p,\ 2p,\ 3p,\ \ldots,\ \text{and } p^{k-1}p = p^k.$$

Thus, the remaining $p^k - p^{k-1} = p^{k-1}(p-1)$ numbers *are* coprime to p. □

That's great, but it still doesn't help us compute $\varphi(12)$. To compute the totient function in general, we can appeal to the following Theorem.

Theorem 5

The totient function is *multiplicative*: if n and m are coprime, then $\varphi(nm) = \varphi(n)\varphi(m)$.

Proof. Consider the map

$$f : \mathbb{Z}/(nm)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, [k]_{nm} \mapsto ([k]_n, [k]_m).$$

We show that this map is well defined. To see this we note that

$$[a]_{mn} = [b]_{mn} \iff mn|a-b \implies m|a-b \textit{ and } n|a-b \iff [a]_m = [b]_m \textit{ and } [a]_n = [b]_n$$
$$\implies ([a]_m, [a]_n) = ([b]_m, [b]_n).$$

This map is injective—if $([k]_n, [k]_m) = ([k']_n, [k']_m)$, we have $n \mid (k-k')$ and $m \mid (k-k')$, together implying that $nm \mid (k-k')$ and $[k]_{nm} = [k']_{nm}$.

Since the domain and codomain both have nm elements, we know f must also be surjective. Thus f is bijective.

Now we know that $\gcd(k, nm) = 1$ iff $\gcd(k, n) = \gcd(k, m) = 1$, so f is a bijection when restricted to

$$\{k \in \mathbb{Z}/(nm)\mathbb{Z} : \gcd(x, nm) = 1\} \to \{(x, y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : \gcd(x, n) = \gcd(y, m) = 1\}.$$

Thus the number of elements in the two sets are equal. □

Example 6 — $\varphi(12) = \varphi(2^2) \cdot \varphi(3) = 2^{2-1}(2-1) \cdot (3-1) = 2 \cdot 2 = 4$. Great, it works!