Lecture 11: Basic number theory

Nitin Saxena [⋆]

IIT Kanpur

1 Euclid's GCD (Contd.)

In general, the equations in the algorithm will look like,

$$
\begin{aligned}
\gcd(a,b) &\to a = q_1 \times b + r_1 \\
\gcd(b,r_1) &\to b = q_2 \times r_1 + r_2 \\
&\vdots \\
\gcd(r_{k-2},r_{k-1}) &\to r_{k-2} = q_k \times r_{k-1} + r_k \\
\gcd(r_{k-1},r_k) &\to r_{k-1} = q_{k+1} \times r_k + 0 \\
\gcd(r_k,0) &\to r_k .
\end{aligned}
\tag{1}
$$

In this case $\gcd(a,b)$ will be r_k.

Notice that $r_{k-1} \geq r_k$, $r_{k-2} \geq r_{k-1} + r_k, \cdots$, $b \geq r_1 + r_2$ and $a \geq b + r_1$. This reminds one of Fibonacci recurrence. Indeed this observation can be used to bound the number of steps k.

Coming from the other direction, r_1 can be written as an *integer linear combination* of a, b, i.e., $r_1 = c_1 a + c_2 b$ for some integers c_1, c_2 using the first equation. Similarly r_2 can be written as an integer combination of b, r_1 and hence a, b.

Keeping track of these coefficients (i.e. by induction), ultimately we can write the $\gcd(a,b) = r_k$ as the integer combination of a, b.

Theorem 1 (Bézout's identity). *For integers a, b, there exist integers α, β, such that,*

$$\gcd(a,b) = \alpha \cdot a + \beta \cdot b \,.$$

It is clear from the argument before that these coefficients can be obtained by keeping track of coefficients in Euclid's algorithm. This is called the *extended Euclidean algorithm.* You can write the extended Euclidean pseudocode as an exercise.

Exercise 1. What can you say about the size of α, β ? Are they unique?

Proof. Wlog assume $a > b > 0$. In that case, the GCD is a positive number.

For convenience we will work with the *coprime* numbers $a' := a/\gcd(a,b)$ and $b' := b/\gcd(a,b)$. The above identity can be written as:

$$1 \;=\; \alpha a' + \beta b' \,.$$

We can ensure $0 \leq \alpha < b'$, by dividing α by b' (say $\alpha = qb' + r$), using the remainder (r) and accordingly changing β (to $\beta - qa'$). Then, $|\beta b'| = |\alpha a' - 1| \leq |b'a'|$. Thus, $|\beta| \leq a'$.

Finally, suppose that α, β in the above range are not unique. Then,

$$(\alpha_1 - \alpha_2) \cdot a' \;=\; (-\beta_1 + \beta_2) \cdot b' \,.$$

By Lemma 1, we get that $b' | (\alpha_1 - \alpha_2)$. Since the difference is smaller than b', we deduce it to be zero. Hence, $(-\beta_1 + \beta_2)$ is also zero. This contradiction implies the uniqueness of (α, β) in the range $[0, \ldots, b' - 1] \times [-a', \ldots, a']$.

$\square$

[⋆] Edited from Rajat Mittal's notes.

Using Theorem 1, we can prove the following lemma.

Lemma 1. *Let* $\gcd(a, b) = 1$. *If* $a \mid bc$ *then* $a \mid c$.

Proof. We know that there exist k, ℓ, such that,

$$1 = ka + \ell b\,.$$

Multiplying both sides by c, we get

$$c = kac + \ell bc\,.$$

Since a divides both the terms on the right hand side, a divides c too. $\square$

References

1. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.
2. P. J. Cameron. Combinatorics: Topics, Techniques and Algorithms. *Cambridge University Press*, 1994.
3. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.