Sketch of Lecture 3 Tue, 8/27/2019

Lemma 15. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d \in \mathbb{N}$. We need to show that $d|a$ and $d|b$ iff $d|r$ and $d|b$. [**iff** is short for "if and only if"]

Equivalently, assuming that $d|b$, we need to show that $d|a$ iff $d|r$.

Indeed, it follows from $\frac{a}{d} = \frac{qb + r}{d} = \frac{qb}{d} + \frac{r}{d}$ that $\frac{a}{d} \in \mathbb{Z}$ iff $\frac{r}{d} \in \mathbb{Z}$. □

Example 16. Using this lemma to compute $\gcd$'s is referred to as the **Euclidean algorithm**.

(a) $\underbrace{\gcd(30, 108)}_{108 = 3 \cdot 30 + 18} = \underbrace{\gcd(18, 30)}_{30 = 1 \cdot 18 + 12} = \underbrace{\gcd(12, 18)}_{18 = 1 \cdot 12 + 6} = \underbrace{\gcd(6, 12)}_{12 = 2 \cdot 6 + 0} = 6$

Alternatively, taking a shortcut by allowing negative remainders:

$\underbrace{\gcd(30, 108)}_{108 = 4 \cdot 30 - 12} = \underbrace{\gcd(12, 30)}_{30 = 2 \cdot 12 + 6} = \underbrace{\gcd(6, 12)}_{12 = 2 \cdot 6 + 0} = 6$

(b) $\underbrace{\gcd(16, 25)}_{25 = 1 \cdot 16 + 9} = \underbrace{\gcd(9, 16)}_{16 = 1 \cdot 9 + 7} = \underbrace{\gcd(7, 9)}_{9 = 1 \cdot 7 + 2} = \underbrace{\gcd(2, 7)}_{7 = 3 \cdot 2 + 1} = \gcd(1, 2) = 1$

Alternatively, again, taking a shortcut by allowing negative remainders:

$\underbrace{\gcd(16, 25)}_{25 = 2 \cdot 16 - 7} = \underbrace{\gcd(7, 16)}_{16 = 2 \cdot 7 + 2} = \underbrace{\gcd(2, 7)}_{7 = 3 \cdot 2 + 1} = \gcd(1, 2) = 1$

Theorem 17. **(Bézout's identity)** Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by.$$

Proof. We proceed iteratively:

$$\begin{array}{rcl}
a & = & q_1 b + r_1, \quad 0 < r_1 < b \\
b & = & q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\
 & \vdots & \\
r_{n-3} & = & q_{n-1} r_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} \\
r_{n-2} & = & q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} & = & q_{n+1} r_n + 0
\end{array}$$

Along the way, we have $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$ (why is it obvious that the last gcd is r_n?).

By the second-to-last equation, $\gcd(a, b) = r_n = r_{n-2} - q_n r_{n-1}$ is a linear combination of r_{n-2} and r_{n-1}. Then, moving one up, we replace r_{n-1} with $r_{n-3} - q_{n-1} r_{n-2}$ to write $\gcd(a, b)$ as a linear combination of r_{n-3} and r_{n-2}. Continuing in that fashion, we ultimately obtain $\gcd(a, b)$ as a linear combination of a and b. □

Let us revisit the previous example to illustrate how the Euclidean algorithm provides us with a way to write $\gcd(a, b)$ as an integer linear combination of a and b.

Example 18. Find $d = \gcd(30, 108)$ as well as integers r, s such that $d = 30r + 108s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{llll}
\gcd(30, 108) & \boxed{108} = 4\cdot\boxed{30} - 12 & \text{or:} & \boxed{A}\quad 12 = -1\cdot\boxed{108} + 4\cdot\boxed{30}\\
= \gcd(12, 30) & \boxed{30} = 2\cdot\boxed{12} + 6 & & \boxed{B}\quad 6 = 1\cdot\boxed{30} - 2\cdot\boxed{12}\\
= \gcd(6, 12) & \boxed{12} = 2\cdot\boxed{6} + 0 & & \\
= 6 & & &
\end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$6 \underset{\boxed{B}}{=} 1\cdot\boxed{30} - 2\cdot\boxed{12} \underset{\boxed{A}}{=} 1\cdot\boxed{30} - 2(-1\cdot\boxed{108} + 4\cdot\boxed{30}) = 2\cdot\boxed{108} - 7\cdot\boxed{30}$$

In summary, we have $2\cdot 108 - 7\cdot 30 = 6$.

Example 19. Find $d = \gcd(16, 25)$ as well as integers r, s such that $d = 16r + 25s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{llll}
\gcd(16, 25) & \boxed{25} = 2\cdot\boxed{16} - 7 & \text{or:} & \boxed{A}\quad 7 = -1\cdot\boxed{25} + 2\cdot\boxed{16}\\
= \gcd(7, 16) & \boxed{16} = 2\cdot\boxed{7} + 2 & & \boxed{B}\quad 2 = 1\cdot\boxed{16} - 2\cdot\boxed{7}\\
= \gcd(2, 7) & \boxed{7} = 3\cdot\boxed{2} + 1 & & \boxed{C}\quad 1 = \boxed{7} - 3\cdot\boxed{2}\\
= 1 & & &
\end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{C}}{=} \boxed{7} - 3\cdot\boxed{2} \underset{\boxed{B}}{=} 7\cdot\boxed{7} - 3\cdot\boxed{16} \underset{\boxed{A}}{=} -7\cdot\boxed{25} + 11\cdot\boxed{16}$$

In summary, we have $-7\cdot 25 + 11\cdot 16 = 1$.

Example 20. **(extra)** Find $d = \gcd(17, 23)$ as well as integers r, s such that $d = 17r + 23s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{llll}
\gcd(17, 23) & \boxed{23} = 1\cdot\boxed{17} + 6 & \text{or:} & \boxed{A}\quad 6 = 1\cdot\boxed{23} - 1\cdot\boxed{17}\\
= \gcd(6, 17) & \boxed{17} = 3\cdot\boxed{6} - 1 & & \boxed{B}\quad 1 = -1\cdot\boxed{17} + 3\cdot\boxed{6}\\
= 1 & & &
\end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{B}}{=} -1\cdot\boxed{17} + 3\cdot\boxed{6} \underset{\boxed{A}}{=} -4\cdot\boxed{17} + 3\cdot\boxed{23}$$

In summary, we have $1 = -4\cdot 17 + 3\cdot 23$.

2 Primes

Lemma 21. **(Euclid's lemma)** If $d|ab$ and $\gcd(a, d) = 1$, then $d|b$.

Proof. Since $(a, d) = 1$, we can find x, y so that $ax + dy = 1$.
We then see that $b = abx + bdy$ is divisible by d (because $d|ab$). □

Definition 22. An integer $p > 1$ is a **prime** if its only positive divisors are 1 and p.

Lemma 23. If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof. If $p|a$, then we are done. Otherwise, $p\nmid a$. In that case, $\gcd(a, p) = 1$ because the only positive divisors of p are 1 and p. Our claim therefore is a special case of the previous lemma. □

Corollary 24. If p is a prime and $p|a_1 a_2 \cdots a_r$, then $p|a_k$ for some $k \in \{1, 2, \ldots, r\}$.

Example 25. This property is unique to primes. For instance, $6|8\cdot 21$ but $6\nmid 8$ and $6\nmid 21$.

Whereas, $2|8\cdot 21$ and, indeed $2|8$. Similarly, $3|8\cdot 21$ and, indeed $3|21$.

Theorem 26. (Fundamental Theorem of Arithmetic) Every integer $n>1$ can be written as a product of primes. This factorization is unique (apart from the order of the factors).

Proof. Let us first prove, by (strong) induction, that every integer $n>1$ can be written as a product of primes.

- **(base case)** $n=2$ is a prime. There is nothing to do.
- **(induction step)** Suppose that we already know that all integers less than n can be written as a product of primes. We need to show that n can be written as a product of primes, too.

  Let $d>1$ be the smallest divisor of n. Then d is necessarily a prime (because if $a>1$ divides d, then a also divides n so that $a=d$ because d is the smallest number dividing n).

  If $d=n$, then n is a prime, and we are already done.

  Otherwise, $\frac{n}{d}>1$ is an integer, which, by the induction hypothesis, can be written as the product of some primes $p_1\cdots p_r$. Then, $n=dp_1\cdots p_r$.

Finally, let us think about why this factorization is unique. Suppose we have two factorizations

$$n=p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

By the corollary, each p_i divides one of the q_j's (and vice versa), in which case $p_i=q_j$, so we can cancel common factors until we see that both factorizations are identical. □

Comment. Have a look at Lecture #1 for some illustration that the idea of factorization into primes and the uniqueness of such factorizations should not be taken entirely for granted.

The executive summary is that, when instead of integers a we work with "generalized integers" such as $a+bi\sqrt{5}$, with $a,b\in\mathbb{Z}$, then factorization is not unique: for instance, we have two different factorizations of 6, namely,

$$6=2\cdot 3,\quad 6=(1+i\sqrt{5})(1-i\sqrt{5}),$$

and the numbers 2, 3, $1\pm i\sqrt{5}$ cannot be factored further.

Example 27. $140=2^2\cdot 5\cdot 7$, $2016=2^5\cdot 3^2\cdot 7$, 2017 is a prime, $2018=2\cdot 1009$, $2019=3\cdot 673$

How can we check that 2017 is indeed prime? Well, none of the small primes $2,3,5,7,11$ divide 2017. But how far do we need to check? Since $\sqrt{2017}\approx 44.91$, we only need to check up to prime 43. (Why?!)