(SF2736, Discrete maths, ht15: L2, Mon 2 Nov 2015)

More about the integers, $\mathbb{Z}$

Definition: ("dual" of gcd) If $m, n \in \mathbb{Z}$ a **least common multiple**, lcm (Sw. mgm), of m and n is a $g \in \mathbb{Z}$ such that

i) $m \mid g, n \mid g$ ii) $m \mid h, n \mid h \Rightarrow g \mid h$ iii) $g \geq 0$

Proposition: For all $m, n \in \mathbb{Z}$, $\mathrm{lcm}(m, n)$ exists uniquely and

$$\boldsymbol{\mathrm{lcm}(m,n) \cdot \gcd(m,n) = m \cdot n.}$$

The **linear Diophantine** (i.e., we want integer solutions x, y) **equation**

$$\boldsymbol{ax + by = c, \qquad a, b, c \in \mathbb{Z}}$$

is solvable **iff** $\gcd(a, b) \mid c$.

In that case (if not $m = n = 0$ and) if $d = \gcd(a, b) = ma + nb$ with $m, n \in \mathbb{Z}$ **all** solutions of the equation are given by $\begin{cases} x = \frac{c}{d}m + \frac{b}{d}k \\ y = \frac{c}{d}n - \frac{a}{d}k \end{cases}, \quad k \in \mathbb{Z}.$

The "normal" method to solve such an equation is to do as in the proof of the proposition, i.e., find $\gcd(m, n) = d$ (using the Euclidean algorithm), divide the equation by d, express 1 as a linear combination of the coefficients of (the new) equation and multiply with its rhs to find an integer solution. **Euler's method** (not treated in the book) includes the rhs from the start and usually leads to smaller numbers in the first solution.

Say, for instance, that we want all integer solutions of the equation $108x + 33y = 78$.

The Euclidean algorithm: $108 = 3 \cdot 33 + 9$, $33 = 3 \cdot 9 + 6$, $9 = 1 \cdot 6 + 3$, $6 = 2 \cdot 3 + 0$, so $d = \gcd(108, 33) = 3$ and there exist solutions. So we go on to find them.

Division by d gives the equivalent equation $36x + 11y = 26$, where $\gcd(36, 11) = 1$.

The "normal" method:

From the above: $36 = 3 \cdot 11 + 3$, $11 = 3 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, $(2 = 2 \cdot 1 + 0)$ and "backwards" that gives $1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = -11 + 4 \cdot 3 = -11 + 4(36 - 3 \cdot 11) = 4 \cdot 36 - 13 \cdot 11$.

Multipying by 26 we see that $x_0 = 4 \cdot 26 = 104$, $y_0 = (-13) \cdot 26 = -338$ solve the equation.

If x, y solve it, we get $36(x - x_0) + 11(y - y_0) = 26 - 26 = 0$, so $36(x - x_0) = -11(y - y_0)$ and $11 \mid (x - x_0)$ (since $\gcd(11, 36) = 1$), $x = x_0 + 11k$, $k \in \mathbb{Z}$. Then $y - y_0 = -36k$ and insertion shows that these x, y solve the equation for all $k \in \mathbb{Z}$.

Euler's method:

Solve for the unknown with the (in absolute value) least coefficient: $y = \frac{26}{11} - \frac{36x}{11} = 2 - 3x + \frac{4-3x}{11}$. x, y form an integer solution iff x and $z = \frac{4-3x}{11}$ are integers, so iff $x, z \in \mathbb{Z}$ with $3x + 11z = 4$, i.e., $x = \frac{4}{3} - \frac{11z}{3} = 1 - 3z + \frac{1-2z}{3}$, so iff $z, u = \frac{1-2z}{3}$ are integers, i.e., iff $z, u \in \mathbb{Z}$ with $2z + 3u = 1$, i.e., $z = -u + \frac{1-u}{2}$, so iff $u, k = \frac{1-u}{2}$ are integers, so $u = 1 - 2k$, with $k \in \mathbb{Z}$ arbitrary.

Insertion gives $z = -(1 - 2k) + \frac{1-(1-2k)}{2} = -1 + 3k$, $x = 1 - 3(-1 + 3k) + \frac{1-2(-1+3k)}{3} = 5 - 11k$ and $y = 2 - 3(5 - 11k) + \frac{4-3(5-11k)}{11} = -14 + 36k$.

Both methods give the same solutions (with different k, $k_{\mathrm{normal}} = -k_{\mathrm{Euler}} - 9$).

The Fundamental theorem of arithmetic:

Every integer ≥ 1 can be written as a product of primes in a unique way (apart from the order of the factors). (1 is "the empty product".)

[The proof of the theorem relies "only" on the possibility of division with a remainder "smaller" than the denominator. Therefore the corresponding theorem of unique (almost) faktorization is true also for polynomials and Gaussian integers (in these cases the faktorizations may differ in the order of the factors and factors which are constants or $1, i, -1, -i$ respectively (like we could have extra factors ± 1 in formulating the theorem for all integers)).]

If $m = p_1^{s_1} \dots p_k^{s_k}, n = p_1^{t_1} \dots p_k^{t_k}$ (where the p_i are different primes)

$$m \mid n \text{ iff } s_i \leq t_i \text{ for all } i = 1, \dots, k \text{ and}$$

$$\gcd(m, n) = p_1^{\min(s_1,t_1)} \dots p_k^{\min(s_k,t_k)}, \quad \mathrm{lcm}(m, n) = p_1^{\max(s_1,t_1)} \dots p_k^{\max(s_k,t_k)}.$$

Modular arithmetic

$$\boldsymbol{x \equiv y \pmod{m}}, \quad \text{or} \quad \boldsymbol{x \equiv_m y}$$

means $m|(x-y)$ and is read "x is congruent to y modulo (or mod) m".

The set of all integers, $\mathbb{Z}$, is partitioned into m classes of congruent numbers:

$$[0]_m = \{0, \pm m, \pm 2m, \dots\},$$
$$[1]_m = \{1, \pm m + 1, \pm 2m + 1, \dots\},$$
$$\vdots$$
$$[m-1]_m = \{-1, \pm m - 1, \pm 2m - 1, \dots\}.$$

The set of these sets ("the integers mod m"): $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$.

Proposition: $x_1 \equiv_m x_2,\ y_1 \equiv_m y_2 \ \Rightarrow\ x_1 + y_1 \equiv_m x_2 + y_2,\ x_1 \cdot y_1 \equiv_m x_2 \cdot y_2$.

So we can **define** $+$ and $\cdot$ on $\mathbb{Z}_m$:

$$[a]_m \circ [b]_m = [a \circ b]_m \quad \text{for} \quad \circ = +, \cdot$$

We usually write $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ and calculate with $+$ and $\cdot$ "as usual but taking remainders mod m".

Definition: $r \in \mathbb{Z}_m$ is **invertible** iff there is $x \in \mathbb{Z}_m$ with $rx = 1$ in $\mathbb{Z}_m$.
Such an x is called r^{-1}, the **inverse** of r.

Theorem: $r \in \mathbb{Z}_m$ is invertible iff $gcd(r, m) = 1$ (in $\mathbb{Z}$).

$rx = 1$ in $\mathbb{Z}_m$ iff $rx - km = 1$ for some $k \in \mathbb{Z}$, so r^{-1} can be found using the Euclidean algorithm ($1 = \gcd(r, m) = ar + bm$ gives $r^{-1} = a$).