(SF2736, Discrete maths, ht15: L1, Mon 2 Nov 2015)

About the integers, $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$

Theorem (division with remainder): If $a, b \in \mathbb{Z},\ b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ with

$$a = bq + r \text{ and } 0 \leq r < |b|.$$

The number q is the **quotient** of a and b, r is (the principal) **remainder**.

[(r is the least number which is ≥ 0 and can be written $a - by,\ y \in \mathbb{Z}$). In fact, most of the corresponding is true for **polynomials** (with rational, real or complex coefficients), where the degree of the remainder, $\deg r(x)$, $<$ the degree of the denominator, $\deg b(x)$, and for **Gaussian integers** (complex numbers $m + in$ $(m, n \in \mathbb{Z})$), where $|r|^2 < |b|^2$.]

To write a natural number in base t, where $t \geq 2$:
By the theorem above we find for any natural number x

$$\begin{cases} x &= q_0 t + r_0 \\ q_0 &= q_1 t + r_1 \\ \vdots & \qquad\qquad\qquad 0 \leq r_i < t \\ q_{n-1} &= q_n t + r_n, \qquad q_n = 0 \text{ (for some } n) \end{cases}$$

so $x = ((\dots((r_n t + r_{n-1})t + r_{n-2})t + \dots + r_2)t + r_1)t + r_0 =$
$= r_n t^n + r_{n-1} t^{n-1} + \dots + r_2 t^2 + r_1 t + r_0,$
i.e. x expressed in base t is $x = (r_n r_{n-1} \dots r_2 r_1 r_0)_t$.

Definition: If $d, m \in \mathbb{Z}$ "$\boldsymbol{d}$ **divides** $\boldsymbol{m}$", "d is a divisor of m", "m is a multiple of d" etc, in symbols $\boldsymbol{d \mid m}$, that there is a $q \in \mathbb{Z}$ such that $m = dq$ (i.e. (if $d \neq 0$) that division of m by d gives remainder 0).

Definition: A **prime** is an integer $p > 1$ which only has the divisors $\pm 1, \pm p$.

Definition: If $m, n \in \mathbb{Z}$ a **greatest common divisor**, gcd (Sw. sgd), of m and n is a $d \in \mathbb{Z}$ such that

i)	$d \mid m, d \mid n$	common divisor
ii)	$c \mid m, c \mid n \Rightarrow c \mid d$	"greatest"
iii)	$d \geq 0$	gives (as it turns out) uniqueness

(Biggs has $c \mid m, c \mid n \Rightarrow c \leq d$ instead of ii), iii). That gives the same, **except** when $m = n = 0$.)

Theorem: For all $m, n \in \mathbb{Z}$ (for Biggs: except $m = n = 0$) there is a unique greatest common divisor $\boldsymbol{d = \gcd(m, n)}$ and $\boldsymbol{d = am + bn}$ for some $a, b \in \mathbb{Z}$.

m and n have the same common divisors as n and $m - nq$, $q \in \mathbb{Z}$, so $\boldsymbol{\gcd(m, n) = \gcd(n, m - nq)}$. By repeating one finds $\gcd(d, 0) = d$, so d, a, b are found using the **Euclidean algorithm** $(n > 0)$ $(\gcd(m, n) = \gcd(n, m) = \gcd(\pm m, \pm n).)$

$$\begin{array}{ll} m = nq_1 + r_1 & 0 \leq r_1 < n \\ n = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & 0 \leq r_{k-1} < r_{k-2} \\ r_{k-2} = r_{k-1} q_k + 0 & \end{array}$$

which gives $\boldsymbol{\gcd(m, n) = r_{k-1}}$.

The second equation from below gives $d = r_{k-1}$ expressed in r_{k-2} and r_{k-3}, r_{k-2} from the equation before is inserted etc, giving $d = am + bn$, some $a, b \in \mathbb{Z}$.

Corollary: If $d, m, n \in \mathbb{Z},\ d \mid mn$ and $\gcd(d, m) = 1$, then $d \mid n$.

(If $\gcd(d, m) = 1$, d and m are said to be **coprime** or **relatively prime**.)