Lecture 5 GCD Algorithm / Primes / Modular arithmetic.

Recall: $S = \{ax+by \in \mathbb{N} \mid x,y \in \mathbb{Z}\}$
least element $d = GCD(a,b)$ ← Bezout's thm

Example: $n = 72$ $m = 60$ $d = (n,m)$.
Note: $d|m$, $d|n \Rightarrow d|n-mq = r$
$72 = 60 \cdot 1 + 12$ $q = \lfloor \frac{72}{60} \rfloor$ $r = 12 = n - mq$.
$(72,60) = (60,12)$ ✓ (greatest integer)
$60 = \boxed{12}\,5 + 0$ $q = \lfloor \frac{60}{12} \rfloor$ $r = 0 = n - mq$.
$(n,m) = m$ if $m|n$
GCD is 12.

Prop: (1) Let $m|n$ then $(n,m) = m$ ($(1,m) = 1$ so...)
(2) $(n,m) = (n-m,m)$ $(n > m)$.

Proof: (1) Let $d = (n,m) \Rightarrow d|m$ (d is divisor). ✓
$m|m$ and $m|n \Rightarrow m|d$ (since greatest) ✓
Thus $d = m$. (both are positive).
(2) Let $(n,m) = d$, $(n-m,m) = d'$
then $d|n, d|m \Rightarrow d|n-m$, $d|m \Rightarrow d|d'$
$d'|n-m$, $d'|m \Rightarrow d'|n-m+m = n$.
So d' is a common divisor. Thus $d'|d$. ✓

So $d'|d$ and $d|d' \Rightarrow d = d'$. □

Remark: If $n = mq + r$. By iteration we see that $(n,m) = (m,r)$.

Algo 1 for computing GCD
steps
1. $n = mq_1 + r_1$ $(r_1 = n, r_0 = m)$ $q_1 = \lfloor \frac{n}{m} \rfloor$ = Greatest integer $\leq \frac{n}{m}$.
2. $m = r_1 q_2 + r_2$ $r_0 = r_1 q_2 + r_2$ $q_2 = \lfloor \frac{m}{r_1} \rfloor$ = Floor of $\frac{m}{r_1}$
$r_1 = r_2 q_3 + r_3$
$r_2 = r_3 q_4 + r_4$
$r_{n-2} = r_{n-1} q_n + r_n$ ← Process stops when $r_n = 0$.
$r_1 > r_2 > \dots > r_n$. This is a decreasing sequence of numbers. For some n, r_n has to be 0. Say $r_n = 0$.
Then $d = r_{n-1}$ (by (1) above).

Remark: By taking $n - qm = r$ instead of just $n - m$ we are trying to speedily find d. What happens if its never better? Sp q's are all 1. Consider $n = F_k$ $m = F_{k-1}$

$F_k = 1 \cdot F_{k-1} + F_{k-2}$
$F_{k-1} = F_{k-2} + F_{k-3}$
⋮

Start with $F_0 = 0$, $F_1 = 1$
Seq is 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...
This is the Fibonacci Sequence. We will find a formula later.
Note. To compute this it's better to keep track of numbers found rather than use recursion every time. "Dynamic programming" This is why @cached_function is used.

Prop. Sp $(a,m) = 1$. Then there is an x s.t. $ax \equiv 1 \pmod m$
Proof: Last time: $ax + by = c$ has a sol. if $(a,b) | c$.
Result follows taking $b = m$, $c = 1$. □ Euler's Totient function.
Def: If a is invertible in $\mathbb{Z}_m$, it is called a unit. $\mathbb{Z}_m^\times = \{\text{set of units in } \mathbb{Z}_m\}$ $\#\mathbb{Z}_m^\times = \phi(m)$

Prop. (Wilson's theorem). p is a prime iff (if and only if) $(p-1)! \equiv -1 \pmod p$
Proof: $(p-1)! = 1 \cdot 2 \cdot 3 \cdots p-1$.
- In $\mathbb{Z}_p$: For every $a \neq 0$, there is a b s.t. $a \cdot b = 1$. ($\mathbb{Z}_p$ is a field).
- $p-1$ is even so can pair them. Are they different?
$x^2 \equiv 1 \pmod p \Rightarrow (x-1)(x+1) \equiv 0 \pmod p$
Recall: $ab \equiv 0 \pmod p \Rightarrow a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$
$\Rightarrow x-1 \equiv 0$ or $x+1 \equiv 0 \Rightarrow x = 1, -1 (= p-1)$.
So $1 \cdot 2 \cdots p-2\,p-1 \equiv p-1 \equiv -1 \pmod p$. □.
(pairs give 1)
. We have shown: if p prime $(p-1)! \equiv -1 \pmod p$.
- Conversely: if m is not a prime then $\exists\, a, b < m$ s.t. $ab \equiv 0 \pmod m$. then $(m-1)! \not\equiv 0 \pmod p$.
So if $(m-1)! \equiv -1$, m cannot be composite, so a prime. □.
Remark: The world's most primality test!
Remark. $P \Rightarrow Q$. If P then Q
Converse: $Q \Rightarrow P$.
$P \iff Q$: $P \Rightarrow Q$, $Q \Rightarrow P$. P if and only if Q

Prop: Let $a_1 \equiv a_2 \pmod m$, $b_1 \equiv b_2 \pmod m$, $c \in \mathbb{Z}$, $m, n \in \mathbb{N}$.
(1) $a_1 + b_1 \equiv a_2 + b_2 \pmod m$
(2) $a_1 b_1 \equiv a_2 b_2 \pmod m$
(3) $ca_1 \equiv ca_2 \pmod m$
(4) $a_1^n \equiv a_2^n \pmod m$.
Proof: Ex. Shows various operations are well defined.

Prop: (Cancellation) Let $(k,m) = d$. If $ka \equiv kb \pmod m$ then $a \equiv b \pmod{\frac{m}{d}}$

Proof: There is an x s.t. $k(a-b) = mx$. Let $m = dm_1$, $k = dk_1$
We get, on cancelling d. $k_1(a-b) \equiv m_1 x$. So $(m_1, k_1) = 1$
Now k_1 has an inverse mod m_1. i.e. $a - b = m_1(x k_1^{-1})$
$\Rightarrow a \equiv b \pmod{m_1}$.

Remark: When $m = p$, a prime, $(k,p) = 1$
$ka \equiv kb \pmod p \Rightarrow a \equiv b \pmod p$.

Prop: (Fermat's little theorem) Let p be a prime, $(a,p) = 1$ (i.e. $p \nmid a$). then $a^{p-1} \equiv 1 \pmod p$.

Proof: Recall (ex): $a, 2a, 3a, \dots, (p-1)a$ are distinct mod p. (since $ma \equiv na \Rightarrow m \equiv n \pmod p$)
Consider $1 \cdot 2 \cdots p-1 \equiv a \cdot 2a \cdot 3a \cdots (p-1)a \pmod p$
$\equiv a^{p-1}(p-1)! \pmod p$
Note $p \nmid (p-1)! \Rightarrow 1 \equiv a^{p-1} \pmod p$ (can cancel)
b/c $(p, (p-1)!) = 1$. □.

Remark: One quick test whether a number is possibly a prime is using Fermat's little theorem. However, converse is not true.

Fermat conjectured $2^{2^n} + 1$ is a prime. These are called Fermat #s. 1, 5, 17, 257, 65537 ← all primes.
$F_5 = 2^{2^5} + 1$ ← Euler showed
$2^{2^5} + 1 \equiv 0 \pmod{641}$. ← Ex → Keep trying all seem to get on this how Euler were. Don't see soln.

Theorem: Let $p | ab$. Then $p|a$ OR $p|b$. (Most imp. prop of prime)
Proof: To prove A or B, we assume not A and prove B. That's enough
Sp $p \nmid a$, $ab \equiv 0 \pmod p$
$\Rightarrow (a^{-1}a)b \equiv 0 \pmod p$ (since $(a,p) = 1, \dots$)
$\Rightarrow b \equiv 0 \pmod p$
$\Rightarrow p|b$. □.

Remark: We got all our results from last weeks theorem when there is a solution of $ax + by = c$. Shows how important that is (important = useful!)
Pending: How to find x, y s.t. $ax + by = c$. A bit later.

Prop: Every # can be written as a product of primes.
Proof: Ex (work HOP.)
Thm. (Fundamental Theorem of Arithmetic) Any $n \in \mathbb{N}, n > 1$, can be written as a product of primes in an (essentially) unique way. $n = p_1^{a_1} \cdots p_k^{a_k}$ for primes $p_1, \dots, p_k$
Proof: Ex. from Prop + Induction. $a_i > 0$.