Math 451

Crypto extended euclidean algorithm

$\operatorname{mod}(\underbrace{a \cdot \bar{a}}, n) = 1$

inverses under multiplication with mod n

$\gcd(a,b) \rightarrow a = q \cdot b + r$

$\gcd(a,b) = \gcd(b,r)$

Bezout's thm $\gcd(a,b) = s \cdot a + t \cdot b$

s, t are integers.

ex if $\gcd(a,b) = 1$ S is a's inv. under mod b

So $1 = \boxed{s \cdot a + t \cdot b}$

$\rightarrow \operatorname{mod}(s \cdot a + \cancel{t \cdot b}^{0}, b) = \operatorname{mod}(1, b)$

$\operatorname{mod}(s \cdot a, b) = 1$

$\gcd(a,b) = \gcd(b, r_1) \quad a = q_1 b + r_1$

$\gcd(b, r_1) = \gcd(r_1, r_2) \quad b = q_2 r_1 + r_2$

$\gcd(r_1, r_2) = \gcd(r_2, r_3) \quad r_1 = q_3 r_2 + r_3$

$$\boxed{r_i} = q_i \boxed{r_{i+1}} + 0$$

gcd

$$\boxed{a = q\,b + 0}$$

$\to$ gcd $= b$

else $r \neq 0$

$$\gcd = \gcd(b, r)$$

$$a = q\,b + 0 \qquad \gcd(a,b) = s \cdot a + t \cdot b$$

$$\gcd(a,b) = \boxed{b = \underbrace{(0)}_{s}a + \underbrace{(1)}_{t}b}$$

$$[g \;\; s1 \;\; t1] = \text{mygcd}(b, r)$$

have
$$\boxed{g = s1 \cdot b + t1 \cdot r}$$
$$a = q \cdot b + r$$

want $g = s \cdot a + t \cdot b$

$g = s1 \cdot b + t1 \cdot r$ with $r = (a - q\,b)$

$$g = s_1 \cdot b + t_1(a - qb)$$

$$g = \underbrace{t_1}_{s} \cdot a + \underbrace{(s_1 - t_1 q)}_{t} b$$

ex

```
octave:6> [g s t] = mygcd(13,5)
g =  1
s =  2
t = -5
```

$\rightarrow \quad 1 = \underbrace{(2)(13)} + \cancel{(-5)(5)}$

2 = 13's inv. mod 5

Speed issues. div_mod

See video

```
function [q r] = div_mod(a,d)
% 'Fast' floating point version ...
% doesn't handle as large of numbers, but
% for what you are given speed is more important
pa = abs(a);

q = floor(pa/d);

r = pa - q*d;

if a < 0 && r ~= 0
  q = -(q + 1);
  r = d - r;
elseif a < 0 && r == 0
  q = -q;
end

end
```