Math 451

proj. 6 → on blackboard.

→ write centrality.m

djk.m ← given (see previous lectures)

Number theory Set: integers ↑ (int64, uint64) ops: +, −, *

division algorithm: div, mod

div_mod as floats $a = q \cdot d + r$ (q: div, r: mod)

$$q = \lfloor a/d \rfloor$$
$$r = a - q*d$$

div_mod using +, −

function [q r] = div_mod(a, d) (a is positive)

```
q = 0;
r = a;
while r >= d
    q = q + 1;
    r = r - d;
end
end
```

pos or neg

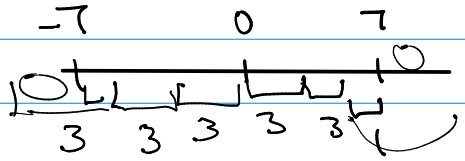
```
function [q r] = div-mod (a,d)
    q = 0;
    r = abs(a);
    while r >= d
        q = q + 1;
        r = r - d;
    end
    if a < 0
        q = -(q+1);
        r = d - r;
    end
end
```

$-6 = (-2)4 + 2$ (q, r)

$6 = (1)4 + 2$

$-7 = (-3)3 + 2$

$7 = (2)3 + 1$



Mod function:

$$\text{mod}(a+b, n) = \text{mod}(\text{mod}(a,n) + \text{mod}(b,n), n)$$

$$\text{mod}(a \cdot b, n) = \text{mod}(\text{mod}(a,n) \cdot \text{mod}(b,n), n)$$

---

base b expansions

$$(1,2,3)_{10} = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

$$(1,0,0,1)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$(2,3,0,4)_7 = 2 \cdot 7^3 + 3 \cdot 7^2 + 0 \cdot 7^1 + 4 \cdot 7^0$$

$$(a_2, a_1, a_0)_b = a_2 \cdot b^2 + a_1 \cdot b + a_0$$

$n = (a_2 a_1 a_0)_b = a_2 \cdot b^2 + a_1 \cdot b + a_0$

$n = a_2 b^2 + a_1 b + a_0$

$n = (a_2 b + a_1) \cdot b + a_0$

$n = q \cdot b + r$

div_mod(n, b)

$q = a_2 b + a_1$

$r = a_0$

$n_2 = a_2 b + a_1$

div_mod(n_2, b)

$q = a_2 \rightarrow n_3$

$r = a_1$

$n_3 = a_2 + 0$

function [a] = base_b(n, b)

```
q = n;
k = 1;
while q ~= 0
  [qk rk] = div_mod(q, b)
    q = qk;
    a(k) = rk;
    k = k+1;
end
a = fliplr(a);
end
```

engine of R.S.A. $a^b \bmod m$

$\Rightarrow (a \cdot a \cdot a \cdot a \cdot \dots \cdot a) \bmod m$

b-times

Function [pm] = power_mod(a, b, m)

pm = 1;

For i = 1:b

pm = mod(a * pm, m);

end

end

---

base b $(a_k b^{k-1} + a_{k-1} b^{k-2} + \dots + a_1 b + a_0)$

$((2)3 + 0)3 + 2$

$((0 \cdot 3 + 2) \cdot 3 + 0) 3 + 2$