MAT 311 LECTURE 3

HENSEL'S LEMMA
PRIMITIVE ROOTS

SIMPLE ENCRYPTION SCHEME

SUPPOSE m IS A POSITIVE INTEGER, $(a,m)=1$. LET $k, \bar{k}$ SATISFY

$$k\bar{k} \equiv 1 \bmod \varphi(m).$$

THEN $a^{k\bar{k}} \equiv a \bmod m$.

PROOF: WRITE $k\bar{k} = 1 + r\varphi(m)$.

RECALL FERMAT'S LITTLE THM SAYS $a^{\varphi(m)} \equiv 1 \bmod m$.

$$a^{r\cdot\varphi(m)+1} \equiv a^1 \cdot (a^{\varphi(m)})^r$$
$$\equiv a \bmod m.$$

ENCRYPTION SCHEME:

a - SOME MESSAGE
n BITS LONG (ASCII CODE)

$m = p_1 p_2$ PRODUCT OF TWO PRIMES, $m > a$.
p_1, p_2 ARE SECRET.

k = A LARGE INTEGER (PUBLIC KEY).

MESSAGE: $b \equiv a^k \bmod m$.

ALICE $\xrightarrow[\text{MESSAGE}]{}$ BOB

EVE

SECRET KEY HELD BY BOB:
$\bar{k}$: $k \cdot \bar{k} \equiv 1 \bmod m$.

TO DECRYPT:

BOB CALCULATES $a \equiv b^{\bar{k}} \bmod m$.
THIS RELIES ON FACTORING m IS BELIEVED TO BE DIFFICULT, SO IT IS DIFFICULT TO CALCULATE $\bar{k}$.

HENSEL'S LEMMA:

$f(x)$ – POLYNOMIAL IN $\mathbb{Z}[x]$.
(INT. COEFFICIENTS)

$f(a) \equiv 0 \mod p^j$.

$f'(a) \not\equiv 0 \mod p$.

THEN THERE IS A UNIQUE $t \mod p$ SUCH THAT
$f(a+tp^j) \equiv 0 \mod p^{j+1}$.

PROOF: NOTICE THAT THE MONOMIAL

$$X \xrightarrow{f} X^r$$

HAS DERIVATIVES

$$f' = r X^{r-1}$$
$$f'' = r(r-1) X^{r-2}$$
$$\vdots$$
$$f^{(k)} = r(r-1)\cdots(r-k+1) X^{r-k}$$

IF $k \leq r$

BY A THEOREM FROM LECTURE 4, $k! \mid r(r-1)\cdots(r-k+1)$

THUS IF WE CONSIDER THE TAYLOR EXPANSION

$$P(x+t) = P(x) + \frac{P'(x)}{1!}\cdot t + \frac{P''(x)}{2!} t^2 + \cdots + \frac{P^{(k)}(x)}{k!} t^k$$

THIS EXPRESSION IS A FIN. SUM IF P IS A POLYNOMIAL; EACH OF THE COEFFICIENTS

$$\frac{P^{(j)}(x)}{j!}$$ IS AN INTEGER.

WRITE

$$f(a+tp^j) = f(a) + t\cdot p^j f'(a) + (tp^j)^2 \frac{f''(a)}{2!} + \cdots + (tp^j)^k \frac{f^{(k)}(a)}{k!} \quad (*)$$

$$\equiv f(a) + t\cdot p^j f'(a) \bmod p^{j+1}$$

THUS $f(a+tp^j) - f(a) \equiv tp^j f'(a) \bmod p^{j+1}$.

RECALL $f(a) \equiv f(a+tp^j) \equiv 0 \bmod p^j$.

$$\frac{f(a+tp^j) - f(a)}{p^j} \equiv t f'(a) \bmod p.$$

THUS $$t \equiv (f'(a))^{-1} \cdot \frac{f(a+tp^j) - f(a)}{p^j} \bmod p.$$

□

THEOREM: (HENSEL VARIANT)

LET $f(x) \in \mathbb{Z}[x]$, AND SUPPOSE $f(a) \equiv 0 \bmod p^j$, THAT $p^\tau \| f'(a)$ AND $j \geq 2\tau + 1$.

p^τ IS THE LARGEST POWER OF p DIVIDING $f'(a)$

IF $b \equiv a \bmod p^{j-\tau}$ THEN $f(b) \equiv f(a) \bmod p^j$, AND THERE IS A UNIQUE $t \bmod p$ SUCH THAT $f(a + tp^{j-\tau}) \equiv 0 \bmod p^{j+1}$.

PROOF: WRITE $b = a + tp^{j-\tau}$.

$$f(b) \equiv f(a) + \boxed{tp^{j-\tau} f'(a)} \bmod p^{j+1}$$

SINCE $2(j-\tau) \geq j+1$. $\equiv 0 \bmod p^{j+1}$

ARGUING AS IN HENSEL'S LEMMA ALLOWS TO SOLVE FOR t. □

THEOREM: IF THE DEGREE n OF A POLYNOMIAL $f(x)$ IS $n \geq p$ THEN EITHER

(1) ALL x MOD p HAVE $f(x) \equiv 0 \bmod p$.

(2) THERE IS A POLYNOMIAL $P(x)$, DEGREE $\leq p-1$, VANISHING AT THE ZEROS OF $f(x)$.

PROOF: SUPPOSE (1) DOES NOT HOLD. LET $r_1, r_2, \ldots, r_m$ BE THE ROOTS, $m \leq p-1$.

$$P(x) = (x-r_1)(x-r_2)\ldots(x-r_m).$$

THIS VANISHES AT THE SAME ROOTS. $\square$

THEOREM: $f(x) \equiv 0 \bmod p$ HAS AT MOST $\deg(f)$ SOLUTIONS. (p PRIME).

PROOF: IF $f(r) \equiv 0 \bmod p$ PERFORM POLYNOMIAL DIVISION TO WRITE

$$f(x) = (x-r)\,g(x) + R$$

WHERE $R \in \mathbb{Z}$. THEN $R \equiv 0 \bmod p$, BY EVAL $x = r$. ASSUME INDUCTIVELY $g(x) \equiv 0 \,(p)$ HAS AT MOST $\deg(g) = d-1$ ROOTS. THE CLAIM FOLLOWS. □

THEOREM: LET $f: \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ BE ANY FUNCTION. THEN THERE IS A POLYNOMIAL P, $\deg(P) \leq p-1$,

$$P(x) \equiv f(x) \bmod p$$

FOR ALL x MOD p.

PROOF: CONSIDER

$$\delta_a(x) = 1 - (x-a)^{p-1}$$

KRONECKER δ AT a.

$$\equiv \begin{cases} 1 \mod p & x \equiv a \ (p) \\ 0 \mod p & x \not\equiv a \mod p. \end{cases}$$

THEN FORM

$$P(x) = \sum_{a \bmod p} f(a)\, \delta_a(x)$$

$$P(a) = \sum_{b \bmod p} f(b)\, \delta_b(b) = f(a).$$

THEOREM: IF $d \mid p-1$ THEN $X^d - 1$ HAS EXACTLY d SOLUTIONS.

PROOF: RECALL THE FACTORIZATION

$$(X^{m_1} - 1) = (x^m - 1)(1 + x^m + x^{2m} + \cdots + x^{(n-1)m}).$$

HENCE $(X^d - 1) \mid (X^{p-1} - 1)$.

RECALL, BY FERMAT'S LITTLE THM.

$$(X^{p-1} - 1) = (x-1)(x-2)\cdots(x-(p-1)).$$

HENCE $X^d - 1$ HAS d DISTINCT ROOTS. $\square$

DEFINITION: LET $m > 1$ BE A (POSSIBLY COMPOSITE) MODULUS, AND $(a, m) = 1$.

THE **ORDER** OF a MOD m IS THE LEAST POSITIVE h

$$a^h \equiv 1 \pmod{m}.$$

(SAME DEF'N AS THE ORDER OF AN ELEMENT IN A GROUP.)

LEMMA: IF a HAS ORD h, THEN THOSE POSITIVE k SUCH THAT $a^k \equiv 1 \pmod m$ ARE THE MULTIPLES OF h.

PROOF: BY THE DIVISION ALGORITHM, $k = qh + r$ WITH $0 \leq r < h$.

$$a^k \equiv (a^h)^q \cdot a^r \pmod m$$
$$\equiv a^r \pmod m.$$

SINCE $r < h$ WE MUST HAVE $r = 0$ FOR $a^k \equiv 1 \pmod m$. □

LEMMA: IF a HAS ORD h. a^k HAS ORD $\frac{h}{(h,k)}$.

PROOF: $(a^k)^{\frac{h}{(h,k)}} \equiv a^{\frac{hk}{(h,k)}} \pmod m$

BUT $h \mid \frac{hk}{(h,k)} = [h,k]$.

SO $(a^k)^{\frac{1}{(h,k)}} \equiv 1 \pmod m$.

IF $(a^k)^r \equiv 1 \pmod m$

THEN $h \mid k \cdot r$ SO $\frac{h}{(h,k)} \mid r$. □

LEMMA: IF a HAS ORD h, b HAS ORD k AND $GCD(h,k)=1$ THEN ab HAS ORD $h\cdot k$.

PROOF: $(ab)^{hk} \equiv (a^h)^k \cdot (b^k)^h$
$\equiv 1 \cdot 1 \equiv 1 \bmod m$.

IF $(ab)^r \equiv 1 \bmod m$ THEN
$b^{r\cdot h} \equiv a^{r\cdot h} b^{r\cdot h} \equiv (ab)^{r\cdot h}$
$\equiv 1 \bmod m$.

THUS $k \mid r\cdot h$ SO $k \mid r$.
SIMILARLY $h \mid r$ SO $k\cdot h \mid r$.
□

DEFINITION: A RESIDUE a MOD m, $(a,m)=1$ IS A **PRIMITIVE ROOT** IF $ORD(a)=\varphi(m)$.

- IF A PRIMITIVE ROOT EXISTS $(\mathbb{Z}/m\mathbb{Z})^\times$ IS CYCLIC, GEN BY a.

LEMMA: LET p, q BE PRIMES WITH $q^\alpha \mid (p-1)$. THEN THERE ARE $q^\alpha - q^{\alpha-1}$ RED RESIDUES MOD p, $ORD(q^\alpha)$.

PROOF: A REDUCED RES X MOD p HAS ORDER q^α IF

(1) $X^{(q^\alpha)} \equiv 1 \bmod p$.

(2) FOR $\beta < \alpha$, $X^{(q^\beta)} \not\equiv 1 \bmod p$.

THE SOLUTIONS OF (1) ARE THE ROOTS OF $X^{(q^\alpha)} - 1 \equiv 0 \pmod p$

THERE ARE q^α OF THESE.

THOSE THAT DO NOT SATISFY (2) SOLVE $X^{q^{\alpha-1}} - 1 \equiv 0 \bmod p$.

THERE ARE $q^{\alpha-1}$ OF THESE.

HENCE $q^\alpha - q^{\alpha-1}$ ARE OF ORDER q^α. □

THEOREM: THERE ARE $\varphi(\varphi(p))$ PRIMITIVE ROOTS MODULO PRIME p.

PROOF: WRITE $p-1$ IN PRIME FACTORIZATION

$$(p-1) = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$$

q_i PRIME.

THERE ARE $q_i^{\alpha_i} - q_i^{\alpha_i - 1}$ ELEMENTS OF ORDER $q_i^{\alpha_i}$.

LET X_i HAVE ORDER $q_i^{\alpha_i}$. FORM

$$X = X_1 X_2 X_3 \cdots X_k.$$

$$ORD(X) = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k} = (p-1).$$

THIS SHOWS PRIMITIVE ROOTS EXIST.

HENCE $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ CYCLIC OF ORDER $p-1$.

GENERATORS IS $\varphi(p-1)$. □

DEF'N: IF $(a,p)=1$, AND $X^n \equiv a \bmod p$ HAS A SOLUTION, THEN a IS CALLED AN nTH POWER RESIDUE.

THEOREM: IF p IS PRIME, $(a,p)=1$

$x^n \equiv a \bmod p$ HAS $GCD(n, p-1)$ OR NO SOLUTIONS ACCORDING AS $a^{\frac{p-1}{(n,p-1)}} \equiv 1 \bmod p$.

(EITHER a IS AN nTH POWER RESIDUE AND #SOLNS IS $(n, p-1)$ OR NOT.)

PROOF:

$X \mapsto X^n$ GIVES A MAP $(\mathbb{Z}/p\mathbb{Q})^\times \longrightarrow \mathbb{Z}/\frac{p-1}{(n,p-1)}\mathbb{Z}$

WHICH IS $(n, p-1)$-TO-1 SINCE $(\mathbb{Z}/p\mathbb{Z})^\times$ IS CYCLIC.

THE CONDITION TO BE IN THE IMAGE IS $a^{\frac{p-1}{(n,p-1)}} \equiv 1 \bmod p$. □

COR. IF $(a,p)=1$,
a IS A QUAD RESIDUE
$\iff a^{\frac{p-1}{2}} \equiv 1 \bmod p.$
$\iff x^2 - a \equiv 0 \bmod p$
HAS 2 SOLUTIONS.