Final Exam

THU, Nov 19

exam: 4^{30} - 5^{45} PM

upload work by 6^{15} PM

PDF

format

- as for midterm exams — 75 min
- show-your-work problems — ~ 4
- short answer problems — ~ 12

practice

- review midterm exams
- practice problems + solutions (2 midterms + final)

tools

- calculators allowed — but: show work
- notes allowed — but: watch time

Questions ?

Likely show-your-work problems:

1. Euclidean algorithm, diophantine equation
2. primitive roots
3. CRT: solving quadratic congruence
4. infinite continued fraction, convergents recursively

EG # inv. quadr. residues

of the form $y^2 \pmod n$ for some y

inv. residues mod n $= \phi(n)$

p, q, r distinct primes, odd

inv. quadr. residues mod p
$= \frac{1}{2}\phi(p) = \frac{1}{2}(p-1)$

inv. quadr. residues mod pq
$= \frac{1}{4}\phi(pq) = \frac{1}{4}\phi(p)\phi(q) = \frac{1}{4}(p-1)(q-1)$

$\frac{1}{8}\phi(pqr) = \frac{1}{8}(p-1)(q-1)(r-1)$

$(\pm 6)^2 \pmod{11}$
$\equiv 3$

$y^2 \equiv 3$, $y = 6$

$y^2 \equiv 4$

EG primitive roots mod 77 ?

exist mod: $1, 2, 4, p^r, 2p^r$ (p odd)

$77 = 7 \cdot 11$

mult order $= \phi(77) = \phi(7)\phi(11) = 6 \cdot 10 = \underline{60}$

generalized Euler: $x^{\lambda} \equiv 1 \pmod n$

$\lambda = \operatorname{lcm}(\phi(p_1^{r_1}), \phi(p_2^{r_2}), \dots)$

$n = p_1^{r_1} p_2^{r_2} \cdots$

Here: $\operatorname{lcm}(\phi(7), \phi(11)) = \operatorname{lcm}(6, 10) = \frac{6 \cdot 10}{2} = 30$

EG

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 4$

$2x \equiv 3 \pmod 5$

$3x \equiv 5 \pmod{11}$

$2^{-1} \equiv 3 \pmod 5$

$3^{-1} \equiv 4 \pmod{11}$

$x \equiv -1 \pmod 5$

$x \equiv -2 \pmod{11}$

$$\Rightarrow x \equiv 1 \cdot 4 \cdot 5 \cdot 11 \cdot \underbrace{(4 \cdot 5 \cdot 11)^{-1}_{\bmod 3}}_{1} + 2 \cdot 3 \cdot 5 \cdot 11 \cdot \underbrace{(3 \cdot 5 \cdot 11)^{-1}_{\bmod 4}}_{(-1 \cdot 1 \cdot (-1))^{-1} \equiv 1} + \dots + \dots \pmod{3 \cdot 4 \cdot 5 \cdot 11}$$

$(a \cdot b \cdot c)^{-1} \equiv a^{-1} \cdot b^{-1} \cdot c^{-1}$

EG $46x + 56y = 10$

$\gcd(46, 56) = 2$

$23x + 28y = 5$ (coefficients: 28, -23)

$\cdot 5$

Bezout's identity: $23r + 28s = 1$ ($r = 11$, $s = -9$)

$\text{xgcd}(23, 28) = (1, 11, -9)$ alternative $(1, -17, 14)$

$46x + 56y = 9$

$23x + 28y = \frac{9}{2}$

$\rightsquigarrow$ no integer solutions

particular solution: $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \cdot 11 \\ 5 \cdot (-9) \end{bmatrix}$

general solution: $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \cdot 11 \\ 5 \cdot (-9) \end{bmatrix} + m \begin{bmatrix} 28 \\ -23 \end{bmatrix}$ ($m \begin{bmatrix} 56 \\ -46 \end{bmatrix}$)

$28 = 1 \cdot 23 + 5$

$23 = 5 \cdot 5 - 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2 = -9 \cdot 5 + 2 \cdot 23$ ($5 \cdot 5 - 23$, $28 - 23$)

$= -9 \cdot 28 + 11 \cdot 23$