LEC 10 09/17/99

SOME APPLICATIONS OF NUMBER THEORY

IN THIS LECTURE NUMBERS ARE INTEGERS

Th.1 FOR ALL $a, b > 0$ THERE EXIST x, y SUCH THAT $xa + yb = \gcd(a, b)$

PROOF. THE EUCLIDEAN ALGORITHM $a = 111,\ b = 45$

$111 = 2 \cdot 45 + 21 \quad \Rightarrow 21 = 111 - 2 \cdot 45$

$45 = 21 \cdot 2 + 3 \quad \Rightarrow 3 = 45 - 2 \cdot 21$

$(21 = 7 \cdot 3)$

WALKING BACKWARD

$3 = 45 - 2(111 - 2 \cdot 45) =$

$= 45 - 2 \cdot 111 + 4 \cdot 45 =$

$= 5 \cdot 45 - 2 \cdot 111$

EQUATION $ax \equiv b \pmod m$ IS CALLED LINEAR CONGRUENCE.

$3x \equiv 2 \pmod 5 \quad x = ?$

$3 \cdot 0 \equiv 0 \pmod 5$; $3 \cdot 1 \equiv 3 \pmod 5$; $3 \cdot 2 \equiv 1 \pmod 5$;

$3 \cdot 3 \equiv 4 \pmod 5$; $3 \cdot 4 \equiv 2 \pmod 5 \Rightarrow x \equiv 4$.

GENERAL METHOD OF SOLVING $ax \equiv b \pmod m$ WHEN (a, m) ARE RELATIVELY PRIME.

1. FIND y SUCH THAT $a \cdot y \equiv 1 \pmod m$
2. $x := b \cdot y$. THEN $a \cdot x = aby = ay \cdot b \equiv b \pmod m$.

$3x \equiv 2 \pmod 5$? $3y \equiv 1 \pmod 5$; $y = 2$

$x = 2 \cdot 2 = 4$.

Th.2. $\gcd(a, m) = 1 \Rightarrow \exists y \ \ ay \equiv 1 \pmod m$

PROOF. By Th.1 FOR SOME x, y

$xm + ya = 1$. THEREFORE $ya \equiv 1 \pmod m$

EXAMPLE. $45 \cdot y \equiv 1 \pmod{101}$

$101 = 2 \cdot 45 + 11 \qquad 11 = 101 - 2 \cdot 45$

$45 = 4 \cdot 11 + 1 \qquad 1 = 45 - 4 \cdot 11 = 45 - 4(101 - 2 \cdot 45) =$

$= 9 \cdot 45 - 4 \cdot 101 \equiv 9 \cdot 45 \pmod{101}$

$y = 9$

$45 \cdot 9 = 405 \equiv 1 \pmod{101}$

SYSTEMS OF LINEAR CONGRUENCES

$x \equiv 2 \pmod 3 \qquad x = ?$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

CHINESE REMAINDER THEOREM

$m_1, m_2 \ldots m_n > 0$ PAIRWISE RELATIVELY PRIME

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

HAS A UNIQUE SOLUTION MODULO $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$

PROOF: (EXISTENCE) $M_k = m/m_k$; $\gcd(m_k, M_k) = 1$

$\exists y_k \quad M_k y_k \equiv 1 \pmod{m_k}$

$x := a_1 M_1 y_1 + \cdots + a_n M_n y_n$. INDEED, $m_1 | M_2, M_3, \ldots$

$x \equiv a_i M_i y_i \equiv a_i \pmod{m_i}$

EXAMPLE FROM ABOVE? $M_1 = 5 \cdot 7 = 35$. $M_2 = 3 \cdot 7 = 21$;

$M_3 = 3 \cdot 5 = 15$; $\quad 35 \cdot 2 \equiv 1 \pmod 3$; $\quad 21 \cdot 1 \equiv 1 \pmod 5$

$15 \cdot 1 \equiv 1 \pmod 7 \qquad 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$

HANDLING LARGE NUMBERS

$m_1 = 99 \quad m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 89\ 403\ 930$

$m_2 = 98 \qquad k < m \Rightarrow k$ IS UNIQUELY REPRESENTED BY A 4-TUPLE OF NUMBERS $< m_i < 100$

$m_3 = 97$

$m_4 = 95$

$$\begin{array}{rl} & 123684 = (33, 8, 9, 89) \\ + & 413456 = (32, 92, 42, 16) \end{array} + \ = (65, 2, 51, 10)$$

LARGE N'S $\Rightarrow$ TUPLES OF $N \pmod{m_i}$

OPERATIONS (LIGHT)

HARD, BUT WE DO IT ONCE

RECOVERING RESULTS BY CHINESE REMAINDER THEOREM

$$x = \ldots \Longleftarrow \begin{cases} x = a_1 \pmod{m_1} \\ \quad \cdots \\ x = a_k \pmod{m_k} \\ x < m_1 \cdot m_2 \cdot \ldots \cdot m_k \end{cases}$$

REAL LIFE EXAMPLE: $2^{35}-1,\ 2^{34}-1,\ 2^{33}-1,\ 2^{31}-1,\ 2^{29}-1,\ 2^{23}-1$

OPERATIONS FOR $N < 2^{184}$

FERMAT'S LITTLE THEOREM

p IS PRIME, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

(FURTHERMORE $a^p \equiv a \pmod p$.)

PROOF. $\mathbb{Z}_p^+ = \{1, 2, 3, \dots, p-1\}$ ALL POSSIBLE REMAINDERS $\neq 0$

$a \cdot \mathbb{Z}_p^+ = \{a\cdot 1, a\cdot 2, a\cdot 3, \dots, a\cdot(p-1)\}$ PAIRWISE DIFFERENT

IF $ax \equiv ay \pmod p \Rightarrow a(x-y) \equiv 0 \pmod p \Rightarrow$

$(x>y)$ $\Rightarrow p \mid a(x-y) \Rightarrow p \mid a \vee p \mid (x-y)$

IMPOSSIBLE BY ASSUMPTIONS   IMPOSSIBLE SINCE $0 < x-y < p$

$\prod \mathbb{Z}_p^+ \equiv \prod a \cdot \mathbb{Z}_p^+ \pmod p$

$1\cdot 2\cdot 3 \cdots (p-1) \equiv (a\cdot 1)\cdot(a\cdot 2)\cdots a(p-1) \pmod p$

$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$

$(p-1)!\,(a^{p-1}-1) \equiv 0 \pmod p$

$p \mid (p-1)! \quad \vee \quad p \mid (a^{p-1}-1)$

IMPOSSIBLE SINCE ALL $x \in \mathbb{Z}_p^+$ $0 < x < p$ $\Rightarrow a^{p-1} \equiv 1 \pmod p$

PUBLIC KEY CRYPTOGRAPHY

ENCRYPTION IS PUBLIC - DECRYPTION IS NOT

RSA ENCRYPTION (1976) RIVEST SHAMIR ADELMAN (M.I.T.)

MESSAGE → INTEGER M (EG. a la' CAESAR)

ORIGINAL TEXT

$C = M^e \pmod n$ e, n ARE GIVEN

CIPHERTEXT $n = p\cdot q$; e, $(p-1)(q-1)$ RELAT. PRIME

EXAMPLE: $n = 43\cdot 59 = 2537$; $e = 13$

NOTE THAT $\gcd(e, (p-1)(q-1)) = \gcd(13, 42\cdot 58) = 1$

MESSAGE "STOP" → INTEGER 1819 1415

$C = M^{13} \pmod{2537}$ FOR EACH GROUP OF FOUR

$1819^{13} = ?$

FAST MODULAR EXPONENTIATION

$1819^2 \pmod{2537}$

$1819^4 \pmod{2537}$

$1819^8 \pmod{2537}$

FIVE MULTIPLICATIONS ONLY

$1819^{13} = 1819^{(8+4+1)} = 1819^8 \cdot 1819^4 \cdot 1819 \pmod{2537}$

$= 2081$; $1415^{13} \pmod{2537} = 2189$; C=2081 2182

RSA DECRYPTION: FIND d = INVERSE TO e modulo $(p-1)\cdot(q-1)$

d EXISTS SINCE $\gcd(e, (p-1)\cdot(q-1)) = 1$

$de \equiv 1 \pmod{(p-1)\cdot(q-1)}$

$de \equiv 1 + x\cdot(p-1)\cdot(q-1)$

$C^d = (M^e)^d = M^{de} = M^{1+x(p-1)\cdot(q-1)} =$

$= M\cdot(M^{p-1})^{(q-1)\cdot x} \equiv M \pmod p$ ASSUMING $p \nmid M$

$\equiv 1 \pmod p$ BY FERMA'S LITTLE TH.

$C^d = M\cdot(M^{q-1})^{(p-1)\cdot x} \equiv M \pmod q$

$\equiv 1 \pmod q$

BY THE CHINESE REMINDER TH. $C^d \equiv M \pmod{pq}$

TO KNOW d ONE NEEDS TO FACTOR $n = p\cdot q$

IF n IS A 400-DIGIT NUMBER THEN IT TAKES 10^9 YEARS TO FIND p, q GIVEN n.

HW 2.5: 12 26d,h 36