CS280, Spring 2001	**Handout 10**
February 12, 2001	

1. Reading: K. Rosen *Discrete Mathematics and Its Applications*, 2.5

2. The main message of this lecture:

> **Primes are atoms of arithmetic with many striking properties. Prime factorization is very hard in practice: we can use this observation to encode messages and feel safe when an encryption key becomes public.**

Some useful math first. As before, all the numbers here are integers.

Theorem 10.1. *For all $a, b > 0$ there exist x, y such that $ax + by = gcd(a, b)$.*
Proof. By example, which is here as good as a general case. Consider $a = 111$, $b = 45$. Run the Euclidean algorithm:

$111 = 2 \cdot 45 + 21 \quad \Rightarrow \quad 21 = 111 - 2 \cdot 45$
$45 = 2 \cdot 21 + 3 \quad \Rightarrow \quad 3 = 45 - 2 \cdot 21$
$21 = 7 \cdot 3 \quad \Rightarrow \quad gcd(111, 45) = 3.$

Now walk these computations backward: $3 = 45-2\cdot21 = 45-2\cdot(111-2\cdot45) = 45-2\cdot111+4\cdot45 = 5\cdot45-2\cdot111$. One can see easily, that $gcd(a, b)$ is a linear combination of each pair of remainders appearing in the process of execution of the algorithm.

Corollary 10.2. *If a,b are relatively prime, then there are x,y, such that $ax + by = 1$.*
Example: $gcd(101, 45) = 1$. Find x, y such that $101 \cdot x + 45 \cdot y = 1$. Use the general method from 10.1. By the Euclidean Algorithm, $101 = 2 \cdot 45 + 11,\ 45 = 4 \cdot 11 + 1$. Walking backwards: $1 = 45 - 4 \cdot 11 = 45 - 4(101 - 2 \cdot 45) = 45 - 4 \cdot 101 + 8 \cdot 45 = 45 \cdot 9 - 101 \cdot 4$, $x = -4,\ y = 9$.

An equation $ax \equiv b \pmod{m}$ is called **linear congruence**. Example: $3x \equiv 2 \pmod{5}$, solution $x =?$. Let us try some x's: $3\cdot0 \equiv 0 \pmod{5}$, $3\cdot1 \equiv 3 \pmod{5}$, $3\cdot2 \equiv 1 \pmod{5}$, $3\cdot3 \equiv 4 \pmod{5}$, $3 \cdot 4 \equiv 2 \pmod{5}$. Thus $x = 4$ is a solution, as well as any number $4 + 5k$. Such a method is practical for small m's: try the numbers from 0 to $m - 1$. Sometimes we are not lucky:
$2x \equiv 1 \pmod{4}$ has no solutions, since $2x$ is always even, i.e. is 0 or 2 $\pmod{4}$.

Theorem 10.3. *If $gcd(a, m) = 1$ then $ax \equiv 1 \pmod{m}$ has a solution.*
Proof. By 10.2, find x, y such that $ax + my = 1$. Then x is a solution: $ax \equiv ax + my \equiv \equiv 1 \pmod{m}$. Example: to solve $45x \equiv 1 \pmod{101}$ use the above example $1 = 45\cdot9-101\cdot4 \equiv \equiv 45 \cdot 9 \pmod{101}$, $x = 9$.

Theorem 10.4. *If $gcd(a, b) = 1$ and $a|z$ and $b|z$ then $ab|z$.*
Proof. From the assumptions: $z = ua = vb$, therefore, $a|vb$. Since a, b are relative primes, $a|v$. (Here is a formal justification for such an observation: by 10.2, $ax + by = 1$ for some x, y, hence $vax + vby = v$. Notice, that a divides both vax and vby, therefore, $a|v$.). Furthermore $v = wa$, $z = vb = wab$ and $ab|z$.

The following generalization of 10.4 naturally holds: if $m_1, m_2, \ldots, m_n$ be pairwise relatively prime and $m_i|z$ for all $i = 1, 2, \ldots, n$, then $m_1 \cdot m_2 \cdot \ldots \cdot m_n|z$.

Systems of linear congruences (consider a special case only): find x such that

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 1 \pmod{7}$$

Theorem 10.5. (The Chinese Remainder Theorem)
Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime. Then the system

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
....
$x \equiv a_n \pmod{m_n}$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Proof. For each $k = 1, 2 \ldots, n$ consider $M_k = m/m_k = m_1 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_n$. Note that $gcd(M_k, m_k) = 1$, o.w. some $d > 1$ divides both m_k and M_k, therefore d divides one of m_i for $i \neq k$, and m_i, m_k are not relatively prime. By 10.3, $\exists y_k \; M_k y_k \equiv 1 \pmod{m_k}$. Then $x := a_1 M_1 y_1 + \ldots + a_n M_n y_n$ is a desired solution. Indeed, $m_i | M_j$ for all $i \neq j$, therefore $x \equiv a_i M_i y_i \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}$ for all $i = 1, 2, \ldots, n$. Let us show the uniqueness. Suppose there is another nonnegative $y < m$ such that $y \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, n$. Without loss of generality assume that $x \geq y$ and take the difference $z = x - y$. ¿From the assumptions it follows that $0 \leq z < m$ and $z \equiv 0 \pmod{m_i}$, $i = 1, 2, \ldots, n$. Therefore, $m_i | z$ for all $i = 1, 2, \ldots, n$. By 10.4 (the general form), $m = m_1 \cdot m_2 \cdot m_n | z$, therefore, $z = 0$, i.e. $x = y$.

Example 10.6. To solve the system of congruences preceding 10.5, apply the general method from the proof of 10.5: $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 5 \cdot 7 = 35$, $M_2 = 3 \cdot 7 = 21$, $M_3 = 3 \cdot 5 = 15$, $35 \cdot 2 \equiv 1 \pmod 3$, $21 \cdot 1 \equiv 1 \pmod 5$, $15 \cdot 1 \equiv 1 \pmod 7$, $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv$ $\equiv 23 \pmod{105}$.

Example 10.7. Handling large numbers by their remainders with respect to several smaller relative primes. $m_1 = 99$, $m_1 = 98$, $m_1 = 97$, $m_1 = 95$, $m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 89403930$. Every $k < m$ can be uniquely represented by a 4-tuple of numbers < 100 that are the remainders of k with respect to m_1, m_2, m_3, m_4. $123684 = (33, 8, 9, 89)$, $413456 = (32, 92, 42, 16)$. Therefore, $123684 + 413456 = (65, 2, 51, 10)$. To convert this 4-tuple back to the integer, one has to solve the system of congruences: $x \equiv 65 \pmod{99}$, $x \equiv 2 \pmod{98}$, $x \equiv 51 \pmod{97}$, and $x \equiv 10 \pmod{99}$.

Theorem 10.8. (Fermat's Little Theorem)
If p is a prime which does not divide a then $a^{p-1} \equiv 1 \pmod p$. Furthermore, $a^p \equiv a \pmod p$.

Proof. Consider $\mathbf{Z}_p^+ = \{1, 2, 3, \ldots, p-1\}$ the set of all positive remainders modulo p, and let $a\mathbf{Z}_p^+ = \{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\}$. All elements in the latter set are distinct $\pmod p$. Indeed, let $ax \equiv ay \pmod p$ and $x \geq y$, thus $0 \leq (x - y) < p$. Then $a(x - y) \equiv 0 \pmod p \Rightarrow p | a(x - y) \Rightarrow p | a$ or $p | (x - y)$. The former is impossible by the assumptions of the theorem. Therefore, $p | (x - y)$ and thus $x - y = 0$, i.e. $x = y$. We have established, that $\mathbf{Z}_p^+$ and $a\mathbf{Z}_p^+$ is the same set modulo p, therefore, the products of their elements coincide mod p:

$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \ldots \cdot (a \cdot (p-1)) \pmod p$
$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$, $(p-1)!(a^{p-1}-1) \equiv 0 \pmod p$, thus $p|(p-1)!$ or $p|(a^{p-1}-1)$.

The former is impossible since a prime p cannot divide any positive number $< (p-1)$. Therefore $p | (a^{p-1} - 1)$ and $a^{p-1} \equiv 1 \pmod p$.

Example 10.9. Evaluate $2^{340} \pmod{11}$. By Fermat's Little Theorem, $2^{10} \equiv 1 \pmod{11}$. Therefore $2^{340} = (2^1 0)^{34} \equiv 1^{34} \equiv 1 \pmod{11}$.

RSA encryption. See the slides and/or the textbook.

Homework assignments. (due Friday 02/16).
10A:Rosen2.5-2f; 10B:Rosen2.5-24ab; 10C:Rosen2.5-26di