MA2C03 Mathematics
School of Mathematics, Trinity College
Hilary Term 2016
Lecture 58 (March 30, 2016)

David R. Wilkins

41.9. The Chinese Remainder Theorem

Let I be a set of integers. The integers belonging to I are said to be *pairwise coprime* if any two distinct integers belonging to I are coprime.

Proposition 41.1

Let $m_1, m_2, \ldots, m_r$ be non-zero integers that are pairwise coprime. Let x be an integer that is divisible by m_i for $i = 1, 2, \ldots, r$. Then x is divisible by the product $m_1 m_2 \cdots m_r$ of the integers $m_1, m_2, \ldots, m_r$.

Proof

For each integer k between 1 and r let P_k be the product of the integers m_i with $1 \leq i \leq k$. Then $P_1 = m_1$ and $P_k = P_{k-1} m_k$ for $k = 2, 3, \ldots, r$. Let x be a positive integer that is divisible by m_i for $i = 1, 2, \ldots, r$. We must show that P_r divides x. Suppose that P_{k-1} divides x for some integer k between 2 and r. Let $y = x/P_{k-1}$. Then m_k and P_{k-1} are coprime (Lemma 41.14) and m_k divides $P_{k-1} y$. It follows from Lemma 41.10 that m_k divides y. But then P_k divides x, since $P_k = P_{k-1} m_k$ and $x = P_{k-1} y$. On successively applying this result with $k = 2, 3, \ldots, r$ we conclude that P_r divides x, as required. ∎

Theorem 41.15

(Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_r$ *be pairwise coprime positive integers. Then, given any integers* $x_1, x_2, \ldots, x_r$, *there exists an integer* z *such that* $z \equiv x_i \pmod{m_i}$ *for* $i = 1, 2, \ldots, r$. *Moreover if* z' *is any integer satisfying* $z' \equiv x_i \pmod{m_i}$ *for* $i = 1, 2, \ldots, r$ *then* $z' \equiv z \pmod{m}$, *where* $m = m_1 m_2 \cdots m_r$.

Proof

Let $m = m_1 m_2 \cdots m_r$, and let $s_i = m/m_i$ for $i = 1, 2, \ldots, r$. Note that s_i is the product of the integers m_j with $j \neq i$, and is thus a product of integers coprime to m_i. It follows from Lemma 41.14 that m_i and s_i are coprime for $i = 1, 2, \ldots, r$. Therefore there exist integers a_i and b_i such that $a_i m_i + b_i s_i = 1$ for $i = 1, 2, \ldots, r$ (Corollary 41.3). Let $u_i = b_i s_i$ for $i = 1, 2, \ldots, r$. Then $u_i \equiv 1 \pmod{m_i}$, and $u_i \equiv 0 \pmod{m_j}$ when $j \neq i$. Thus if

$$z = x_1 u_1 + x_2 u_2 + \cdots x_r u_r$$

then $z \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$.
Now let z' be an integer with $z' \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$. Then $z' - z$ is divisible by m_i for $i = 1, 2, \ldots, r$. It follows from Proposition 41.1 that $z' - z$ is divisible by the product m of the integers $m_1, m_2, \ldots, m_r$. Then $z' \equiv z \pmod{m}$, as required. ∎

Example

Suppose we seek an integer x such that $x \equiv 3 \pmod{5}$, $x \equiv 7 \pmod{11}$ and $x \equiv 4 \pmod{17}$. (Note that 5, 11 and 17 are prime numbers, and are therefore pairwise coprime.) There should exist such an integer x that is of the form

$$x = 3u_1 + 7u_2 + 4u_3,$$

where

$$u_1 \equiv 1 \pmod{5} \quad u_1 \equiv 0 \pmod{11}, u_1 \equiv 0 \pmod{17},$$
$$u_2 \equiv 0 \pmod{5} \quad u_2 \equiv 1 \pmod{11}, u_2 \equiv 0 \pmod{17},$$
$$u_3 \equiv 0 \pmod{5} \quad u_3 \equiv 0 \pmod{11}, u_3 \equiv 1 \pmod{17}.$$

Now u_1 should be divisible by both 11 and 17. Moreover 11 and 17 are coprime. It follows that u_1 should be divisible by the product of 11 and 17, which is 187. Now $187 \equiv 2 \pmod{5}$, and we are seeking an integer u_1 for which $u_1 \equiv 1 \pmod{5}$. However $3 \times 2 = 6$ and $6 \equiv 1 \pmod{5}$, and $3 \times 187 = 561$. It follows from standard properties of congruences that if we take $u_1 = 561$, then u_1 satisfies all the required congruences. And one can readily check that this is the case.

Similarly u_2 should be a multiple of 85, given that $85 = 5 * 17$. But $85 \equiv 8 \pmod{11}$, $7 \times 8 = 56$, $56 \equiv 1 \pmod{11}$, and $7 \times 85 = 595$, so if we take $u_2 = 595$ then u_2 should satisfy all the required congruences, and this is the case.

The same method shows that u_3 should be a multiple of 55. But $55 \equiv 4 \pmod{17}$, $13 \times 4 = 52$, $52 \equiv 1 \pmod{17}$ and $13 \times 55 = 715$, and thus if $u_3 = 715$ then u_3 should satisfy the required congruences, which it does.

An integer x satisfying the congruences $x \equiv 3 \pmod{5}$, $x \equiv 7 \pmod{11}$ and $x \equiv 4 \pmod{17}$, is then given by

$$x = 3 \times 561 + 7 \times 595 + 4 \times 715 = 8708.$$

Now the integers y satisfying the required congruences are those that satisfy the congruence $y \equiv x \pmod{935}$, since $935 = 5 \times 11 \times 17$. The smallest positive value of y with the required properties is 293.

41.10. Fermat's Little Theorem

Theorem 41.16 (Fermat's Little Theorem)

Let p be a prime number. Then $x^p \equiv x \pmod p$ for all integers x. Moreover if x is coprime to p then $x^{p-1} \equiv 1 \pmod p$.

We shall give two proofs of this theorem below.

Lemma 41.17

Let p be a prime number. Then the binomial coefficient $\binom{p}{k}$ is divisible by p for all integers k satisfying $0 < k < p$.

Proof

The binomial coefficient is given by the formula $\binom{p}{k} = \dfrac{p!}{(p-k)!k!}$. Thus if $0 < k < p$ then $\binom{p}{k} = \dfrac{pm}{k!}$, where $m = \dfrac{(p-1)!}{(p-k)!}$. Thus if $0 < k < p$ then $k!$ divides pm. Also $k!$ is coprime to p. It follows that $k!$ divides m (Lemma 41.10), and therefore the binomial coefficient $\binom{p}{k}$ is a multiple of p. ∎

First Proof of Theorem 41.16

Let p be prime number. Then

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k.$$

It then follows from Lemma 41.17 that $(x+1)^p \equiv x^p + 1 \pmod{p}$. Thus if $f(x) = x^p - x$ then $f(x+1) \equiv f(x) \pmod{p}$ for all integers x, since $f(x+1) - f(x) = (x+1)^p - x^p - 1$. But $f(0) \equiv 0 \pmod{p}$. It follows by induction on $|x|$ that $f(x) \equiv 0 \pmod{p}$ for all integers x. Thus $x^p \equiv x \pmod{p}$ for all integers x. Moreover if x is coprime to p then it follows from Lemma 41.11 that $x^{p-1} \equiv 1 \pmod{p}$, as required. ∎

Second Proof of Theorem 41.16

Let x be an integer. If x is divisible by p then $x \equiv 0 \pmod{p}$ and $x^p \equiv 0 \pmod{p}$.

Suppose that x is coprime to p. If j is an integer satisfying $1 \leq j \leq p-1$ then j is coprime to p and hence xj is coprime to p. It follows that there exists a unique integer u_j such that $1 \leq u_j \leq p-1$ and $xj \equiv u_j \pmod{p}$. If j and k are integers between 1 and $p-1$ and if $j \neq k$ then $u_j \neq u_k$. It follows that each integer between 1 and $p-1$ occurs exactly once in the list $u_1, u_2, \ldots, u_{p-1}$, and therefore $u_1 u_2 \cdots u_{p-1} = (p-1)!$. Thus if we multiply together the left hand sides and right hand sides of the congruences $xj \equiv u_j \pmod{p}$ for $j = 1, 2, \ldots, p-1$ we obtain the congruence $x^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. But then $x^{p-1} \equiv 1 \pmod{p}$ by Lemma 41.11, since $(p-1)!$ is coprime to p. But then $x^p \equiv x \pmod{p}$, as required. ∎

42. The RSA Cryptographic System

42.1. The Specification of RSA

Theorem 42.1

Let p and q be distinct prime numbers, let $m = pq$ and let $s = (p-1)(q-1)$. Let j and k be positive integers with the property that $j \equiv k \pmod{s}$. Then $x^j \equiv x^k \pmod{m}$ for all integers x.

Proof

We may order j and k so that $j \leq k$. Let x be an integer. Then either x is divisible by p or x is coprime to p. Let us first suppose that x is coprime to p. Then Fermat's Little Theorem (Theorem 41.16) ensures that $x^{p-1} \equiv 1 \pmod{p}$. But then $x^{r(p-1)} \equiv 1 \pmod{p}$ for all non-negative integers r (for if two integers are congruent modulo p, then so are the rth powers of those integers). In particular $x^{ns} \equiv 1 \pmod{p}$ for all non-negative integers n, where $s = (p-1)(q-1)$.

Now j and k are positive integers such that $j \leq k$ and $j \equiv k \pmod{s}$. It follows that there exists some non-negative integer n such that $k = ns + j$. But then $x^k = x^{ns}x^j$, and therefore $x^k \equiv x^j \pmod{p}$. We have thus shown that the congruence $x^j \equiv x^k \pmod{p}$ is satisfied whenever x is coprime to p. This congruence is also satisfied when x is divisible by p, since in that case both x^k and x^j are divisible by p and so are congruent to zero modulo p. We conclude that $x^j \equiv x^k \pmod{p}$ for all integers x. On interchanging the roles of the primes p and q we find that $x^j \equiv x^k \pmod{q}$ for all integers x. Therefore, given any integer x, the integers $x^k - x^j$ is divisible by both p and q. But p and q are distinct prime numbers, and are therefore coprime. It follows that $x^k - x^j$ must be divisible by the product m of p and q (see Proposition 41.1). Therefore every integer x satisfies the congruence $x^j \equiv x^k \pmod{m}$, as required. $\blacksquare$