Saints and Scoundrels and Two Theorems That Are Really the Same

Ezra Brown

Ezra (Bud) Brown (ezbrown@math.vt.edu) grew up in New Orleans and has degrees from Rice University and Louisiana State University. He has been at Virginia Polytechnic Institute and State University since 1969 and is currently Alumni Distinguished Professor of Mathematics. Bud is a frequent contributor to the MAA journals, having won the Pólya Award in 2000, 2002, and 2006. He enjoys singing (from opera to rock and roll), playing jazz piano, solving word puzzles, and, with his wife Jo, kayaking, bicycling, and birding.

This is a story about counting saints, safeguarding secrets from scoundrels, two back-to-back classes, and how some students who were in both classes pointed out that the Chinese remainder theorem (from number theory) and the polynomial interpolation theorem (from numerical analysis) are really the same.

Did you know that these two theorems are the same?

The Chinese remainder theorem is one of the foundational theorems of number theory. It states that if the positive integers $m_1, \ldots, m_n$ are pairwise relatively prime (that is, no two of them have any common factors except 1), then given arbitrary integers $a_1, \ldots, a_n$ there exists a solution $x = X$ to the system of n congruences

$$x \equiv a_i \bmod m_i \text{ for } 1 \leq i \leq n$$

and that solution X is unique except for adding integer multiples of the product $m_1 m_2 \cdots m_n$. The key to this theorem is that if p is a fixed prime and q is any prime except p, then there exist integers s and t such that $sp + tq = 1$. These conditions let us construct formulas for the solution X.

The polynomial interpolation theorem is one of the foundational theorems of numerical analysis. It states that if $x_1, \ldots, x_n$ are distinct real numbers and $y_1, \ldots, y_n$ are arbitrary real numbers, then there exists a polynomial $P(x)$ of degree at most $n - 1$ such that $P(x_i) = y_i$ for $1 \leq i \leq n$ and that polynomial $P(x)$ is unique. The key to this theorem is that if a and b are distinct numbers, then there exist constants s and t such that $s(x - a) + t(x - b) = 1$. The fact that the x_i are distinct lets us construct formulas for the polynomial $P(x)$; one such formula closely resembles the formula obtained from the Chinese remainder theorem.

These two theorems are special cases of a construct in a more general setting and in this paper we describe a scenario—namely, two back-to-back classes—in which students discovered this fact. We end by describing that general setting, in which the key idea is an ability to write 1 in a special way.

http://dx.doi.org/10.4169/college.math.j.46.5.326
MSC: 11A07, 11T71

The saints go marching in—how many are in that number?

Number theory met at noon and the topic was simultaneous congruences. The class was unhappy with the first example from the previous meeting. A direct search for finding the smallest number leaving remainders of 2, 3, and 2 on division by 3, 5, and 7 (respectively), they claimed, would be quicker and easier than a complicated method. I agreed and then wrote the following problem on the board.

> Find the smallest number N that leaves remainders of 521, 607, and 11,213 on division by 193,707,721, 6,695,717,641, and 761,838,257,287, respectively.

An exhaustive search for that smallest N using a billion computers, each able to check a billion cases per second, would take over over 30,000 years. In contrast, a computer algebra system takes a fraction of a second. So, it must use some method other than a direct search, right?

The class seemed to be in general agreement with this.

To illustrate the method, here is a problem that involves slightly larger divisors than 3, 5, and 7 and that concerns the well-known song "When the Saints Go Marching In." To a lover of numbers, the line "Oh, I want to be in that number" is intriguing because *nobody ever says what that number is*. Here we determine that number for a special case.

The saints go marching in and we know four facts about them:

- When they march in by rows of 7, there are 3 left over.
- When they march in by rows of 11, there is 1 left over.
- When they march in by rows of 13, there are 9 left over.
- There are fewer than 1000 saints.

How many saints go marching in?

Using congruence notation, the problem becomes finding the number of saints S such that

$$S \equiv 3 \bmod 7, \quad S \equiv 1 \bmod 11, \quad S \equiv 9 \bmod 13, \quad S < 1000.$$

At this point, we may ask three questions.

1. Is there a solution?
2. If so, how do you find one?
3. If so, is there a nice formula that gives a solution?

We take these one at a time. First, this set of congruences does indeed have a solution and this is guaranteed by one of the great results of number theory, namely the Chinese remainder theorem (CRT).

Theorem 1 (Chinese remainder theorem). *Let $m_1, \ldots, m_n$ be pairwise relatively prime integers (that is, $\gcd(m_i, m_j) = 1$ for $i \neq j$), and let $y_1, \ldots, y_n$ be integers. Then the system of simultaneous congruences*

$$X \equiv y_1 \bmod m_1, \ldots, X \equiv y_n \bmod m_n$$

has a common solution $X = S$ that is unique mod $m_1 \cdots m_n$.

For a proof, see [**2**, pp. 38–39], [**4**, pp. 158–167], or [**5**, pp. 235–244], for example.

This theorem implies that a solution S exists, since 7, 11, and 13 are pairwise relatively prime. Here is how we can actually find S. The first congruence, $S \equiv 3 \bmod 7$, implies that 7 divides $S - 3$, so $S = 3 + 7t$ for some integer t. Substitution into the second congruence and rearranging terms leads to

$$S = 3 + 7t \equiv 1 \bmod 11, \text{ so } 7t \equiv 1 - 3 \equiv 9 \bmod 11.$$

Recall that the Euclidean algorithm finds $g = \gcd(a, b)$ as well as integers x and y such that $ax + by = g$. If $g = 1$, this implies that $ax \equiv 1 \bmod b$. Thus, x is a multiplicative inverse of $a \bmod b$ and we write $x \equiv a^{-1} \bmod b$. As $\gcd(7, 11) = 1$, we know that $7x \equiv 1 \bmod 11$ has a solution. It turns out that $x = 8$ works, so we obtain $t \equiv 8 \cdot 7t \equiv 8 \cdot 9 \equiv 72 \equiv 6 \bmod 11$ so that $t = 6 + 11u$ and

$$S = 3 + 7(6 + 11u) = 45 + 77u.$$

The third congruence becomes $9 \equiv S \equiv 45 + 77u \bmod 13$; however, $77u \equiv 12u \bmod 13$ and we see that $u \equiv 3 \cdot 12 \equiv 10 \bmod 13$. Thus, $u = 10 + 13v$ and, since $7 \cdot 11 \cdot 13 = 1001$, we obtain our final result, namely

$$S = 3 + 7(6 + 11(10 + 13v)) = 3 + 42 + 770 + 7 \cdot 11 \cdot 13v = 815 + 1001v.$$

Thus, for each integer v, the quantity $S = 815 + 1001v$ satisfies all three congruences. Finally, since $S < 1000$, there are $S = 815$ saints in that number.

Proofs of the CRT provide the following general formula for a general solution.

Theorem 2 (Chinese remainder formula). *Given pairwise relatively prime integers $m_1, \ldots, m_n$, and integers $y_1, \ldots, y_n$, define the numbers M and M_i, M_i^* for $1 \le i \le n$ by*

$$M = m_1 m_2 \cdots m_n, \quad M_i = M/m_i, \quad M_i^* \equiv M_i^{-1} \bmod m_i.$$

Then $X = y_1 M_1 M_1^* + \cdots + y_n M_n M_n^*$ is a solution to the system of n congruences $X \equiv y_i \bmod m_i$ that is unique modulo M.

Note that M_i is the product of all m_j for $j \neq i$ so $\gcd(M_i, m_i) = 1$. It follows that M_i has an inverse mod m_i and we call that inverse M_i^*.

We can use the formula to solve the saints problem. Given $S \equiv 3 \bmod 7$, $S \equiv 1 \bmod 11$, and $S \equiv 9 \bmod 13$, set $m_1 = 7$, $m_2 = 11$, and $m_3 = 13$. Then

$$M_1 = 11 \cdot 13 \equiv 4 \cdot 6 \equiv 24 \equiv 3 \bmod 7 \text{ and } M_1^* = 5,$$
$$M_2 = 7 \cdot 13 \equiv 7 \cdot 2 \equiv 14 \equiv 3 \bmod 11 \text{ and } M_2^* = 4,$$
$$M_3 = 7 \cdot 11 = 77 \equiv 12 \bmod 13 \text{ and } M_3^* = 12,$$

and $S = 3 \cdot 143 \cdot 5 + 1 \cdot 91 \cdot 4 + 9 \cdot 77 \cdot 12 \equiv 815 \bmod 1001$ as before. Finally, we see that $815 = 3 + 116 \cdot 7 = 1 + 74 \cdot 11 = 9 + 62 \cdot 13$ satisfies all three congruences.

The key step in verifying the formula is to see that

$$M_i M_i^* \equiv \begin{cases} 1 & \bmod m_i, \\ 0 & \bmod m_j, \text{ for } j \neq i. \end{cases}$$

With that, class was over. I promised to give a proof the next time, the students dispersed, and several of them walked with me to our cryptography class.

Sharing secrets among untrustworthy persons

Cryptography class met at 1:30 and the topic for the day was how to share a secret using threshold schemes. We began with the following example.

You, a zillionaire, have locked your assets in a safe and only you know the combination. You want to share your estate with your seven children. Some of them are good people, but the rest are untrustworthy scoundrels. To make matters worse, they do not get along with each other. You tell them that three or more of them can discover the secret by working together. Otherwise, your estate will go to your favorite niece and nephew, whom your children loathe.

What you, the zillionaire, have just described is a *threshold scheme*.

That is, let n and w be positive integers with $n \leq w$. An (n, w)-*threshold scheme* is a way of sharing a secret number S among w participants such that any n of them can easily reconstruct S but no subset of smaller size can reconstruct S. You, the zillionaire, want a $(3, 7)$-threshold scheme; the secret S is the combination to the safe.

In a secret-sharing scheme, the person with the secret is the *dealer*, the participants are the *players*, and each player is given a distinct *share*. Here is a threshold scheme developed by Adi Shamir (the "S" in RSA) that works as follows. First, the dealer constructs a polynomial $P(x)$ of degree $n - 1$ whose constant term is the secret S. (For you, the zillionaire, the polynomial is the quadratic $P(x) = S + ax + bx^2$.) Then, the dealer hands out shares to each of w players, the ith player's share being a point $(x_i, y_i) = (x_i, P(x_i))$ on the curve.

Table 1. The dealer's shares in a $(3, 7)$-threshold scheme

Player	1	2	3	4	5	6	7
Share	(1, 9)	(2, 13)	(3, 23)	(4, 39)	(5, 61)	(6, 89)	(7, 123)

A call for volunteers produced the required seven students and I handed out the seven shares shown in Table 1. I instructed three students to pool their shares and solve the resulting equations for the polynomial $S + ax + bx^2$. The remaining four were to pair up and do the same thing. Players 1, 4, and 6 pooled their share and obtained the equations

$$S + a + b = 9,$$
$$S + 4a + 16b = 39,$$
$$S + 6a + 36b = 89.$$

Fingers flew over laptops; solving the resulting 3×3 system yielded the polynomial $11 - 5x + 3x^2$ so the secret number turned out to be 11. Any set of three players would come to the same conclusion.

When players 2 and 5 tried this, their two equations in three unknowns yielded the equations $S = 10b - 19$ and $a = -7b + 16$. Their underdetermined system had many solutions and the constant term S could be anything at all. A similar thing happened with players 3 and 7. Finally, if four or more players pool their shares, then the resulting system will be consistent and the players will learn the secret S.

In general, if n cooperating players pool their shares, then they will find the polynomial $P(x)$ and hence its constant term, which is the secret S, but that no fewer players can gain any information about the secret. This is a consequence of the following theorem on passing a polynomial curve through a given set of points.

Theorem 3 (Polynomial interpolation). *Suppose* $(x_1, y_1), \ldots, (x_n, y_n)$ *are points in the plane with the* x_i *distinct. There is a unique polynomial* $P(x)$ *of degree at most* $n-1$ *that passes through each of these points, i.e.,* $P(x_i) = y_i$ *for* $1 \le i \le n$.

For a proof, see [**1**, pp. 105–116], [**5**, pp. 309–316], or [**8**, pp. 179–199].

Here is how the method works. Given the points $(x_1, y_1), \ldots, (x_n, y_n)$ with distinct x-coordinates, we want to find real numbers $a_0, \ldots, a_{n-1}$ such that the system of equations $y_i = P(x_i) = a_0 + a_1 x_i + \cdots + a_{n-1} x_i^{n-1}$ has a unique solution. The resulting $n \times n$ linear system in the unknowns $\{a_i\}$ becomes the matrix equation $V_n \cdot \mathbf{a} = \mathbf{y}$, where

$$V_n = \begin{bmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{bmatrix}, \quad \mathbf{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}.$$

It turns out that the determinant of V_n (known as a Vandermonde matrix) is given by

$$\det V_n = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Since the x_i are distinct, this formula means $\det V_n \neq 0$ so that the system has a unique solution $\{a_0, \ldots, a_{n-1}\}$ and the resulting polynomial is the unique polynomial of degree at most $n-1$ that passes through the given points.

In a serious cryptographic application, the secret S could be an integer of several hundred bits. One chooses a prime q larger than the secret, and all calculations are done in the integers mod q. The coefficients are chosen randomly from the set $\{1, 2, \ldots, q\}$, each number being chosen with probability $1/q$. The x_i are chosen to be distinct mod q, which implies that the coefficient matrix V_n of the resulting $n \times n$ linear system has nonzero determinant mod q.

There is an alternative to finding the polynomial $P(x)$ via matrix algebra, namely a step-by-step method that leads to a formula for the polynomial.

First, we find a polynomial curve $y = P(x)$ that passes through the point (x_1, y_1). Then we modify P so that the curve passes through both (x_1, y_1) and (x_2, y_2). We proceed in this way until we have constructed a polynomial curve that passes through all the given points. We give the details for three points below.

If (x_1, y_1) is a point on the polynomial curve $y = P(x)$, then we have $y_1 = P(x_1)$. When we divide a polynomial $P(x)$ of positive degree by $x - x_1$, the usual long-division process produces a quotient $q(x)$ and a remainder $r(x)$ and, since $x - x_1$ has degree 1, the remainder is a constant r. Thus $P(x) = r + (x - x_1)q(x)$. If we substitute $x = x_1$, then we see that $r = P(x_1) = y_1$ since the second term vanishes. Thus, $P(x) = y_1 + (x - x_1)q(x)$ is a polynomial that passes through (x_1, y_1).

For $x = x_2$ we have $y_2 = P(x_2) = y_1 + (x_2 - x_1)q(x_2)$. Again, the assumption that the x_i are distinct allows us to divide both sides of this equation by $x_2 - x_1$ and so $q(x_2) = (y_2 - y_1)/(x_2 - x_1)$. As before, this implies $q(x) = q(x_2) + (x - x_2)h(x)$ for some polynomial $h(x)$ and so

$$\begin{aligned} P(x) &= y_1 + (x - x_1)(q(x_2) + (x - x_2)h(x)) \\ &= y_1 + (x - x_1)\left(\frac{y_2 - y_1}{x_2 - x_1} + (x - x_2)h(x)\right). \end{aligned}$$

For the third and last point, we use the fact that $y_3 = P(x_3)$ to find the value of $h(x_3)$. Substituting $x = x_3$ leads to the equation

$$h(x_3) = \frac{1}{x_3 - x_2}\left(\frac{y_3 - y_1}{x_3 - x_1} - \frac{y_2 - y_1}{x_2 - x_1}\right).$$

$P(x)$ goes through the three given points whenever $h(x_3)$ is as above, and, in particular, whenever $h(x)$ is constant with this value of $h(x_3)$. From this, we obtain the equation

$$P(x) = y_1 + (x - x_1)\left(\frac{y_2 - y_1}{x_2 - x_1} + \frac{x - x_2}{x_3 - x_2}\left(\frac{y_3 - y_1}{x_3 - x_1} - \frac{y_2 - y_1}{x_2 - x_1}\right)\right).$$

Indeed, $P(x_i) = y_i$ for $i = 1, 2, 3$. If there were a fourth point, we would write $h(x) = h(x_3) + (x - x_3)k(x)$ and use the fact that $y_4 = P(x_4)$ to put (x_4, y_4) on the curve.

A student stated that the above formula for the solution looked too messy, and asked whether there might be a cleaner-looking formula. This led me to ask the class to take that "messy" formula for $P(x)$ and separate out the terms that contain y_1, y_2, and y_3. They found

$$P(x) = y_1\frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} + y_2\frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3\frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}.$$

We see that the term whose coefficient is y_i is equal to 1 if $x = x_i$ and 0 if $x = x_j$ for $j \neq i$. This form of the polynomial generalizes as follows.

Given n points (x_i, y_i) with the x_i distinct, define the *Lagrange interpolating polynomials* $\mathcal{L}_i(x)$ by

$$\mathcal{L}_i(x) = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Now $\mathcal{L}_i(x_j) = 1$ if $j = i$, 0 for $j \neq i$, and the unique polynomial of degree at most $n - 1$ passing through the n points is given by $P(x) = y_1\mathcal{L}_1(x) + \cdots + y_n\mathcal{L}_n(x)$. This expression is called the *Lagrange interpolation formula*.

A student's hand shot up. "Wait a minute. Isn't this just like the Chinese remainder theorem?"

The connection

I asked her to elaborate.

The student, who was in the number theory class, continued, "Look, last hour we did the Chinese remainder theorem in number theory. You wrote out a general solution. This hour, we just did the polynomial interpolation theorem, and again you wrote out a general solution. The solutions to both problems look the same. So, this new theorem is a polynomial version of the Chinese remainder theorem."

The CRT had made an appearance earlier in the cryptography course. I wrote the theorem on the board and said, "This is one more example of the many connections between seemingly different areas of mathematics. In fact, the two theorems really are the same."

How is the polynomial interpolation problem like a system of congruences?

Let a, b, m be integers with $m \neq 0$. The congruence $a \equiv b \bmod m$ is a statement that the integer $a - b$ is an integer multiple of m.

Let $y_1 = P(x_1)$. When we divide $P(x)$ by $x - x_1$, we get a polynomial quotient $q(x)$ and a polynomial remainder $r = P(x_1)$. As we saw earlier, this leads to the equation $P(x) - y_1 = (x - x_1)g(x)$. We can write this equation as a *polynomial congruence*, namely $P(x) \equiv y_1 \bmod (x - x_1)$. This makes sense, because a congruence is a statement that the difference of two quantities is divisible by a third quantity.

In fact, the sum, difference, and product of polynomials are always polynomials. Division of polynomials, like division of integers, is a different story, and so we make a few definitions. (At this point, we note that because our polynomials have coefficients in some arbitrary field, we expect that our polynomial division will involve not only integers but also rational numbers.)

More formally, let $a(x)$ and $b(x)$ be polynomials with, say, rational coefficients and $b(x)$ not the zero polynomial. We say $b(x)$ divides $a(x)$ provided $a(x) = b(x)d(x)$ for some polynomial $d(x)$. For example, let $c(x) = 2x^3 + 3x^2 - 6x - 35$. Factoring $c(x) = (x^2 + 4x + 7)(2x - 5)$ shows that both $2x - 5$ and $x^2 + 4x + 7$ divide $c(x)$. On the other hand, $c(x) = (x - (3/2))(2x^2 + 6x + 3) - 61/2$ so $x - (3/2)$ does not divide $c(x)$. However, the difference $c(x) - (-61/2)$ is divisible by $x - (3/2)$ and we can write this fact as the congruence

$$c(x) \equiv \frac{-61}{2} \bmod \left(x - \frac{3}{2}\right).$$

From this algebra, the remainder theorem tells us that $c(3/2) = -61/2$ and the preceding congruence tells us that the polynomial $y = c(x)$ passes through the point $(3/2, -61/2)$.

We say that $a(x)$ and $b(x)$ are relatively prime if their only common factors are constant polynomials. We may now rewrite the polynomial interpolation theorem in terms of congruences.

Theorem 4 (Polynomial interpolation, revisited). *Suppose* $(x_1, y_1), \ldots, (x_n, y_n)$ *are points in the plane with the* x_i *distinct. Let*

$$P_i(x) = \prod_{j \neq i} (x - x_j) \quad \textit{and} \quad P_i^* = \frac{1}{\prod_{j \neq i} (x_i - x_j)}.$$

Then $\mathcal{L}_i(x) = P_i(x)P_i^*$*, and the unique polynomial of degree at most* $n - 1$ *that passes through those n points is given by*

$$P(x) = y_1 P_1(x) P_1^* + \cdots + y_n P_n(x) P_n^*.$$

For the Chinese remainder theorem, the assumption that the m_j are pairwise relatively prime is essential: It implies that the product M_i is relatively prime to m_i. That means M_i is invertible mod m_i, a fact that is key to using the Chinese remainder formula.

For the polynomial interpolation theorem, the assumption that the x_j are distinct is essential: It implies that

$$\frac{1}{x_i - x_j}(x - x_j) + \frac{1}{x_j - x_i}(x - x_i) = 1$$

so the polynomials $x - x_j$ are pairwise relatively prime. Hence the product $P_i(x)$ is invertible mod $(x - x_i)$ and we may construct the Lagrange interpolating polynomials.

The polynomials $x - x_1, (x - x_1)(x - x_2), \ldots, (x - x_1)(x - x_2)\cdots(x - x_n)$ that turned up the step-by-step solution to the polynomial interpolation problem are the Newton interpolation polynomials, and the Newton interpolation formula for the solution is given by $P(x) = a_0 + (x - x_1)a_1 + \cdots + (x - x_1)\cdots(x - x_{n-1})a_{n-1}$ for certain constants $a_0, \ldots, a_{n-1}$. The Newton interpolation polynomial representation of the solution to the polynomial interpolation theorem corresponds to the solution to the system of n integer congruences obtained by satisfying one congruence at a time.

Table 2 summarizes the close comparison of the two situations. These two theorems are indeed special cases of a more general construct, so next we look at the big picture.

Table 2. Comparing the two problems

problem	solve $x \equiv a_i \bmod m_i$	solve $P(x) \equiv y_i \bmod (x - x_i)$
assume	$\gcd(m_i, m_j) = 1$ if $i \neq j$	$x_i \neq x_j$ if $i \neq j$
existence	Chinese remainder theorem	polynomial interpolation theorem
technique	Euclidean algorithm	polynomial Euclidean algorithm
solving	successive congruences	Newton interpolation polynomials
formula	Chinese remainder formula	Lagrange interpolation formula

What is the big picture here?

The Chinese remainder theorem begins with a system of congruences of the form $x \equiv a \bmod n$ and gives sufficient conditions for the existence of a solution to that system. The big picture takes place in those familiar algebraic systems called rings.

Let R be a commutative ring with unity element 1. Recall that an *ideal* I of R is a subset of R that is closed under addition and subtraction and such that if $a \in I$ and $r \in R$, then $ra \in I$. The set $\{ka : k \in R\}$ is the *ideal generated by* a, written (a). For example, (3) is the ideal of integer multiples of 3 in the ring of integers and $(x - 5)$ is the ideal consisting of all polynomial multiples of $x - 5$ in the ring of polynomials.

The ideals A and B are called *coprime* provided there exist elements $a \in A$ and $b \in B$ such that $a + b = 1$. In $\mathbb{Z}$, the ideals (118) and (267) are coprime because $43 \cdot 118 + (-19) \cdot 267 = 1$. For the polynomials with real coefficients, if a and b are distinct real numbers, then

$$\frac{1}{b-a}(x - a) + \frac{1}{a-b}(x - b) = 1,$$

and so the ideals $(x - a)$ and $(x - b)$ are coprime.

We have one more definition to go. Let I be an ideal of R and let $x, y \in R$. We say that $x \equiv y \bmod I$ provided $x - y$ is an element of I. As is the case with both congruence mod m for the integers and congruence mod $p(x)$ for the polynomials over a field, congruence modulo an ideal is an equivalence relation.

With all of this terminology in mind, here is one way to generalize our theorems.

Theorem 5 (General form of the Chinese remainder theorem). *Let R be a commutative ring with unity and let $A_1, \ldots, A_n$ be pairwise coprime ideals of R. The system of congruences*

$$X \equiv y_1 \bmod A_1, \ldots, X \equiv y_n \bmod A_n$$

has a common solution $X = X_0$ that is unique modulo the intersection $A_1 \cap \cdots \cap A_n$.

Proof. For $i < j$, since A_i and A_j are relatively prime, we can choose $a_{ij} \in A_j$ and $a_{ji} \in A_i$ such that $a_{ij} + a_{ji} = 1$. Then, for all $i \neq j$, we have $a_{ij} \equiv 1 \bmod A_j$ and $a_{ij} \equiv 0 \bmod A_i$. Now set $P_i = \prod_{j \neq i} a_{ij}$ so that $P_i \equiv 1 \bmod A_i$ and $P_i \equiv 0 \bmod A_j$ for all $j \neq i$. Then we can see that $X_0 = \sum_i y_i P_i$ is a solution to the given system of equations.

If X_0' is another solution, then $x_0' - x_0 \equiv 0 \bmod A_i$ for all i. Therefore $X_0' - X_0 \in A_1 \cap \ldots \cap A_n$ as desired. ∎

Finally, we know that if the greatest common divisor of the integers a and b is equal to 1, then we may write 1 as a linear combination of a and b; an analogous result is true for polynomials over a field. That "special way to write 1" is the key to both of our theorems, and coprimality of ideals is the key generalization.

And that is why the Chinese remainder theorem and the polynomial interpolation theorem really are the same theorem.

Coda

Shamir describes his threshold scheme in [**6**] and Stinson gives an excellent treatment of this and other secret-sharing schemes in [**7**, pp. 481–515]. Schroeder [**5**] treats both the Chinese remainder and polynomial interpolation theorems and is an eminently readable treatment of many applications of number theory. For the big picture, a good source is the abstract algebra text by Hungerford [**3**, pp. 131–132].

The CRT finds applications in the areas of error-correcting codes; in cryptography, especially in encryption, authentication, and key agreement protocols; and in algorithms for counting the number of points on elliptic curves—to name just three. Exploring the CRT gives rise to much beautiful mathematics. And as my number theorist colleague Theresa Vaughan (1941–2009) told me many times, "You can go a long way into number theory with only the Euclidean algorithm, the pigeonhole principle, and the Chinese remainder theorem."

Finally, the solution to that problem from the number theory class that involved large numbers is $N = 804{,}155{,}562{,}959{,}699{,}457{,}504{,}628{,}440{,}626$. The computer algebra system Mathematica on my laptop computer found N in 222 microseconds—using, of course, the Chinese remainder theorem!

Summary. The Chinese remainder theorem and the polynomial interpolation theorem are foundational theorems of number theory and numerical analysis, respectively. These two theorems are special cases of a construct in a more general setting and we describe a scenario—namely, two back-to-back classes—in which students can discover this fact. We end by describing that general setting, in which the key idea is an ability to write 1 in a special way.

References

1. R. L. Burden, J. D. Faires, *Numerical Analysis*. Ninth edition. Brooks and Cole, New York, 2011.
2. U. Dudley, *Elementary Number Theory*. Second Edition. Dover, Mineola, NY, 2008.
3. T. W. Hungerford, *Algebra*. Springer, New York, 1974.
4. K. H. Rosen, *Elementary Number Theory and its Applications*. Fifth edition. Pearson/Addison-Wesley, Boston, 2005.
5. M. Schroeder, *Number Theory in Science and Communication*. Fifth edition. Springer, Berlin, 2009.
6. A. Shamir, How to share a secret, *Comm. ACM* **22** (1979) 612–613, http://dx.doi.org/10.1145/359168.359176.
7. D. R. Stinson, *Cryptography: Theory and Practice*. Third edition. CRC, Boca Raton, FL, 2005.
8. E. Süli, D. Myers, *An Introduction to Numerical Analysis*. Cambridge Univ. Press, Cambridge, 2003.

