Collection of rules, techniques and theorems for solving polynomial congruences
11 April 2012 at 22:02

Polynomial congruences come up constantly, even when one is dealing with much deeper problems in number theory which initially seem completely unrelated. Over time I have come across a number of rules, techniques and theorems for solving them, but these are spread out in numerous different places. I thought it would be useful to quickly collect the main ones (with examples) in this note, to have them all in one place for easy reference from now on. I'll deal with linear congruences and simultaneous linear congruences first, then quadratic congruences to prime moduli, quadratic congruences to composite moduli, polynomial congruences of higher degrees, and finally polynomial congruences with prime power moduli.

A key basic idea with congruences is that every integer \( n \) has an associated set of least positive residues, which is the set containing the smallest \( n \) non-negative integers \( \{0, 1, 2, \ldots, n-1\} \) to which every other integer is congruent modulo \( n \). The picture above shows the set of least positive residues for \( n = 13 \).

(Sometimes the set of least absolute residues modulo \( n \) is also useful, which is the set of \( n \) integers to which all other integers are congruent modulo \( n \) and whose largest member in absolute value is the smallest possible. For example, the set of least absolute residues for \( n = 4 \) is \{-1, 0, 1, 2\}, and the set of least absolute residues for \( n = 7 \) is \{-3, -2, -1, 0, 1, 2, 3\}). In general, any set of \( n \) integers is a complete set of residues modulo \( n \) provided no two of them are congruent modulo \( n \).

Example:
Suppose that \( \gcd(a, n) = 1 \). We can easily prove that for any integer \( c \), the \( n \) numbers
\[
c, c + a, c + 2a, \ldots, c + (n-1)a
\]
form a complete set of residues modulo \( n \).

Consider any two distinct numbers from the list \( c, c + a, c + 2a, \ldots, c + (n-1)a \). Denote them by \( c+xa \) and \( c+ya \) where \( x \) and \( y \) are distinct elements of the set of least positive residues modulo \( n \). If they are congruent modulo \( n \) then
\[
c+xa \equiv c+ya \pmod{n}
\]
\[
\rightarrow xa \equiv ya \pmod{n}
\]
\[
\rightarrow x \equiv y \pmod{n}
\]
(Cancellation of \( a \) is allowed since \( \gcd(a, n) = 1 \)). But this is a contradiction since \( x \) and \( y \), being least positive residues modulo \( n \), cannot be congruent to each other modulo \( n \). Therefore no two distinct numbers from the list \( c, c + a, c + 2a, \ldots, c + (n-1)a \) can be congruent modulo \( n \), so the list constitutes a complete set of residues modulo \( n \). QED

A couple of other basic points to note:

A property of congruence that is extremely often used is that if \( a \equiv b \pmod{m} \) and \( a \equiv b \pmod{n} \), where \( \gcd(m, n) = 1 \), then \( a \equiv b \pmod{mn} \).

Another is the basic cancellation rule that if \( ca \equiv cb \pmod{n} \), where \( \gcd(c, n) = 1 \), then \( a \equiv b \pmod{n} \).

--------------------------------------------------------------------------------------------------------------------------

LINEAR CONGRUENCES

Considering first the linear congruence \( ax \equiv b \pmod{n} \), the following rules apply:

1. The congruence has solutions iff \( \gcd(a, n) \) divides \( b \).
2. If \( \gcd(a, n) = 1 \), the congruence has a unique solution.
3. If \( \gcd(a, n) = d \) and \( d \) divides \( b \), then the congruence has \( d \) solutions which are obtained by first finding the unique solution modulo \( n/d \) of the congruence \( (a/d)x \equiv (b/d) \pmod{n/d} \), and then adding multiples \( r(n/d) \) to this solution for \( 1 \leq r < d \).

Example: The congruence \( 12x \equiv 15 \pmod{21} \) is such that \( \gcd(12, 21) = 3 \), so this congruence has 3 solutions which can be obtained by finding the unique solution of the congruence \( 4x \equiv 5 \pmod{7} \). By inspection, the solution is \( x \equiv 3 \pmod{7} \), so the three solutions of the original congruence are \( x \equiv 3 \pmod{21} \), \( x \equiv 10 \pmod{21} \) and \( x \equiv 17 \pmod{21} \). It is possible to formulate a general 'strategy' for quickly solving linear congruences of the type \( ax \equiv b \pmod{n} \) as follows:

1. Check that \( \gcd(a, n) \) divides \( b \). If it does not, the congruence has no solutions. If it does:
2. Cancel any common divisors of all three of \( a \), \( b \) and \( n \). The resulting congruence has a unique solution modulo the new modulus. The resulting coefficients (originally \( a \) and \( b \)) can then be changed by applying the remaining steps below in any order, any number of times, with the goal of reaching a congruence in which the coefficient of \( x \) is 1.
3. Cancel any common divisor of the coefficients.
4. Replace either coefficient by any congruent number.
5. Multiply through the congruence by any number which is relatively prime to the modulus.

Example: To solve \( 9x \equiv 15 \pmod{26} \), we first observe that \( \gcd(9, 26) = 1 \) so the congruence has a unique solution. Multiplying through by 3 we get

\[ 27x \equiv 45 \pmod{26} \]
\[ \leftrightarrow x \equiv 45 \pmod{26} \]
\[ \leftrightarrow x \equiv 19 \pmod{26} \]

Example: To solve \( 18x \equiv 39 \pmod{69} \) we observe that \( \gcd(18, 69) = 3 \) which divides 39, so the congruence has 3 solutions. Dividing through by 3 we get \( 6x \equiv 13 \pmod{23} \). Multiplying through by 4 we get

\[ 24x \equiv 52 \pmod{23} \]
\[ \leftrightarrow x \equiv 52 \pmod{23} \]
\[ \leftrightarrow x \equiv 6 \pmod{23} \]

So the solutions of the original congruence are \( x \equiv 6 \pmod{69} \), \( x \equiv 29 \pmod{69} \), and \( x \equiv 52 \pmod{69} \).

SIMULTANEOUS LINEAR CONGRUENCES

The key theorem underlying the solution of simultaneous linear congruences is the famous 'Chinese Remainder Theorem' which is usually stated as follows:

**Chinese Remainder Theorem**

Let \( n_1, n_2, \ldots, n_r \) be positive integers such that \( \gcd(n_i, n_j) = 1 \) for \( i \neq j \). Then the system of linear congruences

\[ x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}; \quad \ldots; \quad x \equiv b_r \pmod{n_r} \]

has a simultaneous solution which is unique modulo \( n_1n_2\ldots n_r \).

A common situation in which simultaneous linear congruences arise is when trying to solve a single linear congruence with a large composite modulus. The modulus can be broken down into its prime-power factors, and each of these factors then gives rise to a linear congruence which is to be solved simultaneously with the others.

Example: To solve the linear congruence \( 3x \equiv 5 \pmod{1001} \) we first observe that 1001 = \( 7 \times 11 \times 13 \). This gives rise to the three simultaneous linear congruences

\[ 3x \equiv 5 \pmod{7}; \quad 3x \equiv 5 \pmod{11}; \quad 3x \equiv 5 \pmod{13} \]

Solving each of these linear congruences individually we get
The positive integers \( x \) which satisfy the congruence \( x \equiv 6 \pmod{13} \) are
\[ x = 6, 19, 32, 45, 58, 71, 84, 97, \ldots \] (increase by 13 until solution of second congruence is found)

Of these, 97 is the first which is also congruent modulo 11 to 9, so \( x = 97 \pmod{11 \times 13} \) is the unique solution of the final pair of simultaneous linear congruences in the original system.

The positive integers \( x \) which satisfy the congruence \( x \equiv 97 \pmod{11 \times 13} \) are
\[ x = 97, 240, 383, 526, 669, \ldots \] (increase by \( 11 \times 13 \) until solution of first congruence is found)

Of these, 669 is the first which is also congruent modulo 7 to 4, and hence is the smallest positive integer satisfying all three simultaneous linear congruences.
Therefore \( x \equiv 669 \pmod{1001} \) is the unique solution of the original congruence.

QUADRATIC CONGRUENCES TO PRIME MODULI

These are congruences of the form \( ax^2 + bx + c \equiv 0 \pmod{p} \) where \( p \) is an odd prime and \( a \) is not congruent to zero modulo \( p \).

For any such congruence we can always 'complete the square' on the left hand side by multiplying through by \( 4a \). This will not affect the congruence because \( \gcd(4a, p) = 1 \). We get
\[ 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p} \]
\( \leftrightarrow (2ax + b)^2 \equiv b^2 \pmod{p} \)
\( \leftrightarrow (2ax + b) \equiv b \pmod{p} \)
\( \leftrightarrow y \equiv d \pmod{p} \)
where \( y = 2ax + b \) and \( d = b^2 - 4ac \).
Thus, we only need to solve the quadratic congruence \( y^2 \equiv d \pmod{p} \), and then for each solution \( y \) of this we can recover a solution of the original congruence by solving the linear congruence \( 2ax + b \equiv y \pmod{p} \).

The key point is the following: a quadratic congruence to a prime modulus has solutions iff \( b^2 - 4ac \) is congruent modulo \( p \) to a square. In general a quadratic congruence to a prime modulus may have 0, 1 or 2 solutions.

Example: To solve \( 2x^2 + 2x + 1 \equiv 0 \pmod{29} \) we first compute the discriminant, which is -4. The congruence has a solution iff -4 is congruent to a square modulo 29. By inspection we see that \(-4 \equiv 5^2 \pmod{29} \) and \(-4 \equiv (-5)^2 \pmod{29} \). Therefore the congruence does have solutions.
To find these we solve \( 4x + 2 \equiv 5 \pmod{29} \) and \( 4x + 2 \equiv -5 \pmod{29} \).
In the first case we get
\[ 4x \equiv 3 \pmod{29} \leftrightarrow 4x \equiv 32 \pmod{29} \leftrightarrow x \equiv 8 \pmod{29} \]
In the second case we get
\[ 4x \equiv -7 \pmod{29} \leftrightarrow 4x \equiv 22 \pmod{29} \leftrightarrow 2x \equiv 11 \pmod{29} \leftrightarrow 2x \equiv 40 \pmod{29} \leftrightarrow x \equiv 20 \pmod{29} \]
Therefore the original congruence has the two solutions \( x \equiv 8 \pmod{29} \) and \( x \equiv 20 \pmod{29} \).

As shown above, any quadratic congruence to a prime modulus can be reduced to the simple form \( x^2 \equiv a \pmod{p} \) so a lot of attention has been paid to developing techniques for quickly finding solutions to this simplified form. The terminology used is that \( a \) is a quadratic residue of the odd prime \( p \) if \( x^2 \equiv a \pmod{p} \) has a solution (a not equal to zero mod \( p \)). Otherwise \( a \) is a quadratic non-residue of \( p \). (Only odd primes \( p \) are considered. The only quadratic residue of 2 is 1). Whether or not \( a \) is a quadratic residue is referred to as the quadratic character of \( a \).

A key theorem relating to the quadratic residues of any odd prime \( p \) is that there are exactly \((p-1)/2\) quadratic residues and \((p-1)/2\) quadratic non-residues. The quadratic residues are congruent modulo \( p \) to the integers \( 1^2, 2^2, 3^2, \ldots \), \((p-1)/2\)^2. The quadratic non-residues are then the remaining \((p-1)/2\) non-zero numbers in the set of least positive residues of \( p \).
Thus, one way to find the quadratic residues of a given odd prime \( p \) is simply to find the squares of the first \((p-1)/2\) non-zero integers and evaluate them modulo \( p \).

Example: To find the quadratic residues of 11 we observe that \((11-1)/2 = 5\) and evaluate
\[ 1^2 \equiv 1 \pmod{11} \]
\[ 2^2 \equiv 4 \pmod{11} \]
\[ 3^2 \equiv 9 \pmod{11} \]
\[ 4^2 \equiv 16 \equiv 5 \pmod{11} \]
\[ 5^2 \equiv 25 \equiv 3 \pmod{11} \]

Therefore the quadratic residues of 11 are 1, 3, 4, 5 and 9. The remaining non-zero numbers in the set of least positive residues of 11 are the quadratic non-residues, i.e., 2, 6, 7, 8, 10.
Another approach to solving this kind of problem is to use Euler’s Criterion:

**Euler’s Criterion**

Let $p$ be an odd prime and $a \neq 0 \pmod{p}$. Then $a$ is a quadratic residue of $p$ if, and only if, $a^{(p-1)/2} \equiv 1 \pmod{p}$ and is a quadratic non-residue of $p$ if, and only if, $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Example: To determine the quadratic residues of 13, we look at $a^4$ for the first six non-zero least positive residues of 13. Each of these will either be 1 or -1 mod 13, in accordance with Euler’s criterion. If $a$ is a quadratic residue by this test, then so is 13-a, so this enables us to identify all the quadratic residues in the set of least positive residues of 13. We have

1⁴ ≡ 1 (mod 13)
2⁴ ≡ 16 × 4 ≡ 3 × 4 ≡ 12 ≡ -1 (mod 13)
3⁴ ≡ 27 × 27 ≡ 1 (mod 13)
4⁴ ≡ 16 × 16 × 16 ≡ 3 × 3 × 3 ≡ 1 (mod 13)
5⁴ ≡ 25 × 25 × 25 ≡ (-1) x (-1) x (-1) ≡ -1 (mod 13)
6⁴ ≡ 36 × 36 × 36 ≡ (-3) x (-3) x (-3) ≡ -1 (mod 13)

Therefore the quadratic residues are 1, 3, 4, 9, 10, 12, and the quadratic non-residues are 2, 5, 6, 7, 8, 11.

Yet another approach is to use primitive roots. For an odd prime $p$, $r$ is a primitive root of $p$ if $r$ has order $p-1$, i.e., if $p-1$ is the smallest integer such that when $r$ is raised to its power, the result is congruent to 1 modulo $p$. Then the set of integers $\{r, r^2, \ldots, r^{p-1}\}$ is a reduced set of residues for $p$, i.e., after evaluating each of them modulo $p$ we end up with the non-zero least positive residues of $p$, namely $\{1, 2, \ldots, p-1\}$. The even powers of the primitive root $r$ are the quadratic residues of $p$, since they are all squares. There are, of course, $(p-1)/2$ such even powers.

Example: Given that 2 is a primitive root of 19, we can find the quadratic residues of 19 by evaluating the even powers of 2 up to 18 modulo 19:

2² ≡ 4 (mod 19)
2⁴ ≡ 16 (mod 19)
2⁶ ≡ 32 × 2 ≡ 13 × 2 ≡ 26 ≡ 7 (mod 19)
2⁸ ≡ 2⁴ × 2² ≡ 7 × 4 ≡ 28 ≡ 9 (mod 19)
2¹⁰ ≡ 2⁸ × 2² ≡ 9 × 4 ≡ 36 ≡ 17 (mod 19)
2¹² ≡ 2⁶ × 2⁶ ≡ 7 × 7 ≡ 49 ≡ 11 (mod 19)
2¹⁴ ≡ 2¹² × 2² ≡ 11 × 4 ≡ 44 ≡ 6 (mod 19)
2¹⁶ ≡ 2¹⁴ × 2² ≡ 6 × 4 ≡ 24 ≡ 5 (mod 19)
2¹⁸ ≡ 2¹⁶ × 2² ≡ 5 × 4 ≡ 20 ≡ 1 (mod 19)

Therefore the quadratic residues of 19 are 1, 4, 5, 6, 7, 9, 11, 16, and 17, and the quadratic non-residues are 2, 3, 8, 10, 12, 13, 14, 15, 18.

The Legendre symbol is useful as a shorthand for stating a number's quadratic character, and is also useful in calculations. If $p$ is an odd prime and $a$ is not congruent to zero modulo $p$, then the Legendre symbol $(a/p) = 1$ if $a$ is a quadratic residue of $p$, and $(a/p) = -1$ if $a$ is a quadratic non-residue of $p$.

The Legendre symbol obeys the following properties, which are useful to know for calculations:
Properties of the Legendre symbol

Let $p$ be an odd prime and let $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$. Then the following properties hold.

(a) If $a \equiv b \pmod{p}$ then $(a/p) = (b/p)$.
(b) $(a^2/p) = 1$
(c) $(ab/p) = (a/p)(b/p)$
(d) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$
(e) $(-1/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

The quadratic character of 2

If $p$ is an odd prime then

$$(2/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8}, \\ -1, & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}. \end{cases}$$

The Law of Quadratic Reciprocity

If $p$ and $q$ are distinct odd primes then

$$(p/q) = \begin{cases} (q/p), & \text{if either } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -(q/p), & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Example: To work out if the congruence $x^2 + 6x + 11 \equiv 0 \pmod{29}$ has a solution, we calculate its discriminant, which is -8. The congruence has a solution iff -8 is a quadratic residue of 29. Using the Legendre symbol we can work this out as follows:


Thus -8 is a quadratic non-residue of 29 and the given quadratic congruence does not have a solution.

Example: For which odd primes $p \neq 7$ does $(7/p) = 1$?

Using the LQR we have:

Example: To work out if the congruence $3x^2 - 8x - 5 \equiv 0 \pmod{139}$ has a solution, we calculate its discriminant, which is 124. The congruence has a solution iff 124 is a quadratic residue of 139, i.e., iff $(124/139) = 1$. We can use the Legendre symbol to work this out as follows:


Thus 124 is a quadratic residue of 139 and the given quadratic congruence does have a solution.

Example: For which odd primes $p \neq 7$ does $(7/p) = 1$?

Using the LQR we have:
\[(7/p) = (p/7) \text{ if } p \equiv 1 \pmod{4}\]
\[(7/p) = (-1)(p/7) \text{ if } p \equiv 3 \pmod{4}\]

The quadratic residues of 7 are:

- \[1^2 \equiv 1 \pmod{7}\]
- \[2^2 \equiv 4 \pmod{7}\]
- \[3^2 \equiv 2 \pmod{7}\]

i.e. 1, 2, 4, and the quadratic non-residues are 3, 5, 6. Therefore

\[(7/p) = 1 \text{ if:}\]
\[p \equiv 1 \pmod{4} \text{ and } p \equiv 1, 2, 4 \pmod{7}\]
\[p \equiv 3 \pmod{4} \text{ and } p \equiv 3, 5, 6 \pmod{7}\]

Therefore we consider possible values of \(p\) modulo 28 that satisfy the above congruences (only have to consider odd numbers and those which are not divisible by 7). Possible primes modulo 28 are thus:

- \[p \equiv 1 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 1 \pmod{7}\]
- \[p \equiv 3 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 3 \pmod{7}\]
- \[p \equiv 5 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 5 \pmod{7}\]
- \[p \equiv 9 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 2 \pmod{7}\]
- \[p \equiv 11 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 4 \pmod{7}\]
- \[p \equiv 13 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 6 \pmod{7}\]
- \[p \equiv 15 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 1 \pmod{7}\]
- \[p \equiv 17 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 3 \pmod{7}\]
- \[p \equiv 19 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 5 \pmod{7}\]
- \[p \equiv 23 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 2 \pmod{7}\]
- \[p \equiv 25 \pmod{28} \rightarrow p \equiv 1 \pmod{4} \text{ and } p \equiv 4 \pmod{7}\]
- \[p \equiv 27 \pmod{28} \rightarrow p \equiv 3 \pmod{4} \text{ and } p \equiv 6 \pmod{7}\]

So the possible primes are \(p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}\).

Example: For which primes \(p > 3\) is \((6/p) = 1\)?

We use the facts that \((6/p) = (2/p)(3/p)\) and:

- \[(2/p) = 1 \text{ if } p \equiv \pm 1 \pmod{8}\]
- \[(3/p) = 1 \text{ if } p \equiv \pm 1 \pmod{12}\]

We consider possible values of \(p\) modulo \(\text{lcm}(8, 12) = 24\). These are:

- \[p \equiv 1 \pmod{24} \rightarrow p \equiv 1 \pmod{8} \text{ and } p \equiv 1 \pmod{12}\]
- \[p \equiv 5 \pmod{24} \rightarrow p \equiv 5 \pmod{8} \text{ and } p \equiv 5 \pmod{12}\]
- \[p \equiv 7 \pmod{24} \rightarrow p \equiv -1 \pmod{8} \text{ and } p \equiv 7 \pmod{12}\]
- \[p \equiv 11 \pmod{24} \rightarrow p \equiv 3 \pmod{8} \text{ and } p \equiv -1 \pmod{12}\]
- \[p \equiv 13 \pmod{24} \rightarrow p \equiv 5 \pmod{8} \text{ and } p \equiv 1 \pmod{12}\]
- \[p \equiv 17 \pmod{24} \rightarrow p \equiv 1 \pmod{8} \text{ and } p \equiv 5 \pmod{12}\]
- \[p \equiv 19 \pmod{24} \rightarrow p \equiv 3 \pmod{8} \text{ and } p \equiv 7 \pmod{12}\]
- \[p \equiv 23 \pmod{24} \rightarrow p \equiv -1 \pmod{8} \text{ and } p \equiv -1 \pmod{12}\]

Therefore the possible primes are \(p \equiv 1, 5, 19, 23 \pmod{24}\).

Yet another method for determining whether or not an integer is a quadratic residue of an odd prime is Gauss' Lemma, which can be stated as follows:
**Gauss’ Lemma**

Let $p$ be an odd prime and $a \neq 0 \pmod{p}$. Let $S$ be the set

$$S = \left\{ a, 2a, 3a, \ldots, \frac{p-1}{2}a \right\}$$

consisting of the first $\frac{p-1}{2}$ positive multiples of $a$. If $n$ denotes the number of members of $S$ whose least positive residue modulo $p$ exceeds $\frac{p}{2}$, then $(a/p) = (-1)^n$.

Example: To use Gauss’ Lemma to evaluate $(11/19)$, we compute the set

$S = \{11, 22, 33, 44, 55, 66, 77, 88, 99\}$.

We now replace each element of $S$ by its least positive residue modulo 19 and put them in order:

$S' = \{1, 3, 4, 6, 9, 11, 12, 14, 17\}$.

Since four elements of $S'$ exceed $19/2$, Gauss’ Lemma tells us that $(11/19) = (-1)^4 = 1$.

Example: To use Gauss’ Lemma to show that 2 is a quadratic residue of each prime of the form $p \equiv 7 \pmod{8}$, we observe that $p = 8k + 7$ for some positive integer $k$, so the set $S$ in Gauss’ Lemma is of the form

$S = \{2, 4, 6, \ldots, p-1\} = \{2, 4, 6, \ldots, 4k+2, 4k+4, \ldots, 8k+6\}$

The number $n$ in Gauss’ Lemma is the number of elements in the set

$\{4k+4, 4k+6, \ldots, 8k+6\}$

Halving each term in this set we see that $n$ is the number of elements in the set

$\{2k+2, 2k+3, \ldots, 4k+3\}$

Therefore $n = (4k+3) - (2k+2) + 1 = 2k+2$

so $n$ is even and thus $(2/p) = 1$, confirming that 2 is a quadratic residue of $p$.

---

**QUADRATIC CONGRUENCES TO COMPOSITE MODULI**

When the modulus is composite, it can be factored into prime powers, and solutions of the quadratic congruence can be found modulo each of these prime powers by some method (e.g. exhaustion, trying all the least positive residues one by one). Having obtained these solutions, a solution to the original quadratic congruence can then be found by making use of the Chinese Remainder Theorem. The following example illustrates this technique.

Example: To solve $2x^2 + 5x - 3 \equiv 0 \pmod{72}$ we begin by observing that $72 = 2^3 \times 3^2$. We then need to solve

$2x^2 + 5x - 3 \equiv 0 \pmod{8}$ and $2x^2 + 5x - 3 \equiv 0 \pmod{9}$.

Trying all eight possibilities for the first congruence and all nine for the second we find that

$2x^2 + 5x - 3 \equiv 0 \pmod{8}$ has the unique solution $x \equiv 5 \pmod{8}$ and

$2x^2 + 5x - 3 \equiv 0 \pmod{9}$ has solutions $x \equiv 5, 6 \pmod{9}$.

The congruence $2x^2 + 5x - 3 \equiv 0 \pmod{72}$ therefore has two solutions:

(a). the simultaneous solution of $x \equiv 5 \pmod{8}$ and $x \equiv 5 \pmod{9}$, namely $x \equiv 5 \pmod{72}$ and

(b). the simultaneous solution of $x \equiv 5 \pmod{8}$ and $x \equiv 6 \pmod{9}$. The set of numbers which satisfy the second are:

$x = 6, 15, 24, 33, 42, 51, 60, 69, \ldots$

The number 69 is the first one which also satisfies $x \equiv 5 \pmod{8}$, so the unique simultaneous solution is $x \equiv 69 \pmod{72}$.

---

**POLYNOMIAL CONGRUENCES OF HIGHER DEGREES**
First, to clarify what is meant by the 'degree' of a general polynomial congruence, note that the congruence $7x^3 + 4x^2 - 3 \equiv 0 \pmod{7}$ is actually of degree 2, not 3, because the leading term $7x^3$ vanishes modulo 7. Therefore the degree of a polynomial congruence refers to the highest power of $x$ in the polynomial which does not vanish in this way.

Any polynomial congruence can be solved by 'exhaustion', by simply trying all the least positive residues of the modulus, one by one.

It is often possible to simplify the solution of polynomial congruences of high degree by replacing them with ones of smaller degree using Fermat's Little Theorem.

Fermat's Little Theorem says that if $p$ is a prime and $a$ is any integer with $\gcd(a, p) = 1$, then $a^p \equiv a \pmod{p}$.

Example: To solve $x^2 + 3x^4 + 8x^3 + 6 \equiv 0 \pmod{7}$, we could just try all the least positive residues of 7 and see which of them are solutions. However, we can also use FLT which says $x^7 \equiv x \pmod{7}$. Then:

$x^2 \equiv x^7 \times x^7 \times x^7 \equiv x^7 \times x \equiv x^8 \pmod{7}$

Similarly, $x^4 \equiv x^2 \pmod{7}$ and $x^0 \equiv x^4 \pmod{7}$.

Therefore solving the original congruence is equivalent to solving

$x^2 + 3x^2 + 8x^4 + 3x^2 + 6 \equiv 0 \pmod{7}$

= $8x^4 + 7x^2 + 6 \equiv 0 \pmod{7}$

Simplifying further by reducing the coefficients, $8 \equiv 1 \pmod{7}$, etc., we arrive at the equivalent congruence

$x^4 - 1 \equiv 0 \pmod{7}$

Checking the fourth powers of 0, ±1, ±2, and ±3, we find that the congruence has just the two solutions $x \equiv \pm 1 \pmod{7}$.

POLYNOMIAL CONGRUENCES WITH PRIME POWER MODULI

The section above on quadratic congruences to composite moduli showed that when the modulus is composite, it can be factored into prime powers, and solutions of the quadratic congruence can be found modulo each of these prime powers. The overall solution to the quadratic congruence with the composite modulus can then be obtained from these sub-solutions.

This basic idea can also be applied to polynomial congruences of higher degrees. Specifically, the problem of solving a polynomial congruence

$$f(x) \equiv 0 \pmod{m}$$

can be reduced to that of solving a system of congruences

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \quad (i = 1, 2, \ldots, r)$$

where

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

In this section I set out an algorithm, with an accompanying example, for solving polynomial congruences with prime power moduli of the form

$$f(x) \equiv 0 \pmod{p\alpha}$$

Step 1. So suppose we want a solution of the congruence
We begin by first considering the congruence

\[ f(x) \equiv 0 \pmod{p^\alpha} \quad (1) \]

Example: \( x^2 + 3x - 16 \equiv 0 \pmod{81} \)

We begin by first considering the congruence

\[ f(x) \equiv 0 \pmod{p} \quad (2) \]

Example: \( f(x) = x^2 + 3x - 16 \equiv 0 \pmod{3} \)

Step 2. If (2) has no solutions, then (1) has no solutions. If (2) does have solutions, we choose one of these, call it \( r \), which lies in the interval \( 0 \leq r < p \). We compute the following numbers:

- \( f(r) \)
- \( k = f(r)/p \)
- \( f'(r) \)

Example: \( r = 1 \quad f(r) = -12 \)

\[ k = \frac{f(r)}{p} = \frac{-12}{3} = -4 \]

\[ f'(r) = 2r + 3 = 5 \]

Step 3. If \( k \) and \( f'(r) \) are both NOT congruent to 0 modulo \( p \) (as in the above example), then \( r \) can be 'lifted' in a unique way from \( p \) to \( p^2 \), i.e., we can use \( r \) to compute a solution \( a \) of the polynomial congruence

\[ f(x) \equiv 0 \pmod{p^2} \quad (3) \]

Example: \( x^2 + 3x - 16 \equiv 0 \pmod{9} \)

This solution \( a \) of (3) is computed from \( r \) using the formula

\[ a = r + qp \]

where \( q \) satisfies the linear congruence

\[ qf'(r) + k \equiv 0 \pmod{p} \quad (4) \]
Example: $q^5 - 4 \equiv 0 \pmod{3}$

has the unique solution $q = 2$, so

$$a = 1 + 3(2) = 7$$

Thus, in our example, the solution to (3) is $a \equiv 7 \pmod{9}$.

If $k$ is not congruent to 0 modulo $p$, but $f'(r)$ is, then $r$ cannot be lifted to a solution of (3). In this case we begin anew with a different solution $r$. If no $r$ can be lifted, then (3) has no solution.

If $k$ is congruent to 0 modulo $p$ for some $r$, we examine the linear congruence in (4). This collapses to $qf'(r) \equiv 0$ in this case, and thus has:

1 solution $q$ if $f'(r)$ is not congruent to 0 modulo $p$
$p$ solutions $q$ if $f'(r)$ is congruent to 0 modulo $p$

In either case, for each solution $q$ the number $a = r + qp$ gives a solution of (3).

To expand on this a bit more explicitly:

(a). If $f'(r)$ is NOT congruent to 0 mod $p$, then the only value of $q$ such that $0 \leq q < p$ which satisfies the congruence is $q = 0$, in which case $a = r$ is a solution of (3).

(b). If $f'(r)$ is congruent to 0 mod $p$, then any value of $q$ such that $0 \leq q < p$ satisfies the above congruence, and thus there are $p$ solutions $(0, 1, 2, \ldots, p-1)$. For each of these possible choices of $q$, $a = r + qp$ gives a solution of (3).

Step 4. For each solution of (3), we now repeat the entire procedure to find solutions of

$$f(x) \equiv 0 \pmod{p^3} \quad (5)$$

with (3) as the basic starting point.

In our example, we set $r = 7$, since we found this is a solution of (3). We compute:

$f(7) = f(r) = 54$
$k = f(7)/p^2 = 54/9 = 6$
$f'(r) = 2r + 3 = 17$

Neither 17 nor 6 are congruent to 0 modulo $3^2 = 9$, so $r = 7$ can be lifted to a solution $a$ of $x^2 + 3x - 16 \equiv 0 \pmod{27}$

The solution $a$ will be given by

$a = r + qp^2 = 7 + 9q$

where $q$ is the solution to the linear congruence

$17q + 6 \equiv 0 \pmod{9}$

We find this solution to be $q \equiv 6 \pmod{9}$

Therefore the solution to (5) is obtained as

$a = 7 + 9(6) = 61 \equiv 7 \pmod{27}$

Thus, the solution to (5) is $a \equiv 7 \pmod{27}$.

Step 5. For each solution of (5), we now repeat the entire procedure to find solutions of

$$f(x) \equiv 0 \pmod{p^4} \quad (6)$$

with (5) as the basic starting point.
In our example, we set $r = 7$, since we found this is a solution of (5). We compute:

$f(r) = f(7) = 54$

$k = \frac{f(r)}{p^3} = \frac{54}{27} = 2$

$f'(r) = 2r + 3 = 17$

Neither 17 nor 2 are congruent to 0 modulo $3^3 = 27$, so $r = 7$ can be lifted to a solution $a$ of

$x^2 + 3x - 16 \equiv 0 \pmod{81}$

The solution $a$ will be given by

$a = r + qp^3 = 7 + 27q$

where $q$ is the solution to the linear congruence

$17q + 2 \equiv 0 \pmod{27}$

We find this solution to be $q \equiv 11 \pmod{27}$

Therefore the solution to (6) is obtained as

$a = 7 + 27(11) = 304 \equiv 61 \pmod{81}$

Thus, the solution to (6) is $a \equiv 61 \pmod{81}$.

Step 6. In our example, this completes the process in that we have now found one solution of (1) by starting with $r = 1$ in (2). We could find a second solution by starting with $r = 2$ in (1) and following the same procedure. In general, we keep going with the above procedure until all the solutions of (1) have been found.