Chapter 3 of Number Theory with Computer Applications

by Kumanduri and Romero;

University of Windsor 62-322 Course notes by M. Hlynka and W.L. Yee.

MODULAR ARITHMETIC

3.1 Congruences:

Definition 3.1.1: If a, b, m are integers, we say that a is congruent to b modulo m (written as $a \equiv b \, mod \, m$) if $m|(a-b)$. (I.e. a and b leave the same remainder when you divide by m.) Otherwise we write $a \not\equiv b \, mod \, m$.

Example:

$23 \equiv 8 \, mod \, 5$ because $5|(23-8)$

$5^7 \equiv 2 \, mod \, 3$ because $78125 = 3(26041) + 2$ so $3|(78125-2)$.

If $a = qm + r$, then $a \equiv r \pmod{m}$.

Proposition 3.1.3: (p. 61)

(a) $a \equiv a \, mod \, m$

(b) $a \equiv b \, mod \, m$ iff $b \equiv a \, mod \, m$.

(c) $a \equiv b \, mod \, m$ and $b \equiv c \, mod \, m$ imply $a \equiv c \, mod \, m$.

So congruence modulo m is an equivalence relation and divides the integers into equivalence classes depending on the remainder upon division by m.

Proposition 3.1.5 If a, b, c, d are integers, then

(a) $a \equiv b \, (mod \, m)$ implies $ac \equiv bc \, (mod \, m)$

(b) $a \equiv b\,(mod\,m)$ implies $a \pm c \equiv b \pm c\,(mod\,m)$

(c) $a \equiv b\,(mod\,m)$ and $c \equiv d\,(mod\,m)$ imply $ac \equiv bd\,(mod\,m)$

(d) $a \equiv b\,(mod\,m)$ implies $a^k \equiv b^k\,(mod\,m)$ for positive integers k.

Proof.

(a) $a \equiv b\,(mod\,m)$ implies $m|(a-b)$ implies $m|c(a-b) = ca - cb$ so $ca \equiv cb\,(mod\,m)$

(b) exercise

(c) $a \equiv b\,(mod\,m)$ and $c \equiv d\,(mod\,m)$ imply $ac \equiv bc\,(mod\,m)$ and $bc \equiv bd\,(mod\,m)$. Thus, by Proposition 3.1.3.(c), we have $ac \equiv bd\,(mod\,m)$

(d) $a \equiv b\,(mod\,m)$ implies (by (c)) that $a^2 \equiv b^2\,(mod\,m)$. We can continue to multiply both sides in the same way so the result follows.

■

Example What is the remainder when 2^{1234} is divided by 7.

SOLUTION: $2^{1234}\,mod(7) \equiv ?$ Note that $2^1 \equiv 2\,(mod\,7)$; $2^2 \equiv 4\,(mod\,7)$; $2^3 \equiv 8 \equiv 1\,(mod\,7)$. Thus

$2^{1234} \equiv 2^{3(411)+1} \equiv (2^3)^{411}2^1 \equiv 1^{411}2 \equiv 2\,(mod\,7)$.

Example Is the sum of 3 consecutive cubes always divisible by 9?

SOLUTION 1: Let $S = n^3 + (n+1)^3 + (n+2)^3$.

There are 9 cases. All can be checked so the sum is divisible by 9.

If $n \equiv 0(mod\,9)$ then $S \equiv 0^3 + 1^3 + 2^3 \equiv 1 + 8 \equiv 0(mod\,9)$.

If $n \equiv 1(mod\,9)$ then $S \equiv 1^3 + 2^3 + 3^3 \equiv 1 + 8 + 0 \equiv 0(mod\,9)$.

If $n \equiv 2(mod\,9)$ then $S \equiv 2^3 + 3^3 + 4^3 \equiv 8 + 0 + 1 \equiv 0(mod\,9)$.

If $n \equiv 3(mod\,9)$ then $S \equiv 3^3 + 4^3 + 5^3 \equiv 0 + 1 + 8 \equiv 0(mod\,9)$.

etc.

SOLUTION 2: Let

$$\begin{aligned}
S &= (n-1)^3 + n^3 + (n+1)^3 \\
&= (n^3 - 3n^2 + 3n - 3) + n^3 + (n^3 + 3n^2 + 3n + 1) \\
&= 3n^3 + 6n = 3n(n^2 + 2).
\end{aligned}$$

If we can show that $T = n(n^2 + 2)$ is divisible by 3, we are done.
If $n \equiv 0 (mod\, 3)$ then $T \equiv 0(0^2 + 2) \equiv 0(mod\, 3)$.
If $n \equiv 1 (mod\, 3)$ then $T \equiv 1(1^2 + 2) \equiv 0(mod\, 3)$.
If $n \equiv 2 (mod\, 3)$ then $T \equiv 2(2^2 + 2) \equiv 0(mod\, 3)$.
So $T \equiv 0(mod\, 3)$ and so the sum of 3 consecutive cubes is divisible by 9.

Example AAF 104 Number Theory Problems, Example 1.21) Find all primes p and q such that $p + q = (p - q)^3$.
$(p - q)^3 = p + q \neq 0$, so p and q are distinct and thus relatively prime.
Since $p - q \equiv p - q + p + q \equiv 2p \pmod{p + q}$, taking the given equation modulo $p + q$ gives $0 \equiv 8p^3 \pmod{p + q}$. Because p and q are relatively prime, so are p and $p+q$. Therefore $0 \equiv 8 \pmod{p+q}$ so that $p + q$ divides 8. Therefore the only solution is $p = 5, q = 3$.

Divisibility Rules: See exercise 17, p. 68

A positive integer is divisible by 2 if it is even.

A positive integer is divisible by 5 if it ends in 0 or 5.

Divisibility by 3 or 9: Any positive integer can be written as $n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_0$.
Since $10 \equiv 1\, (mod\, 3)$ and $10 \equiv 1\, (mod\, 9)$, it follows that

$n \equiv a_m(1)^m + a_{m-1}(1)^{m-1} + \cdots + a_0 \equiv a_m + \cdots + a_0 \pmod 3$ or $\pmod 9$.

So we can check for divisibility (mod 9) by just adding the digits.

Example: Is 123456789 divisible by 9?

Yes, since the sum of the digits is divisible by 9.

Example: What is the remainder of 2017 when divided by 9?

$2017 \equiv 2+0+1+7 \equiv 10 \equiv 1+0 \equiv 1 \pmod 9$ so the remainder is 1.

Example: 1994 ARML individual question #5. In the addition below, each letter represents a different digit. Compute the digit that J represents.

$$\begin{array}{r} ABC \\ DEF \\ +GHI \\ \hline 1J32 \end{array}$$

The digits A to J are a permutation of 0 to 9. Modulo 9, we have $A+B+C+D+E+F+G+H+I \equiv 1+J+3+2 \pmod 9$ so $45 - J \equiv 6 + J \pmod 9$ so $45 - 6 \equiv 39 \equiv 12 \equiv 2J \pmod 9$ so $J = 6$.

(Some questions from Engel, Problem-Solving Strategies, others from de Koninck, 1001 Problems in Classical Number Theory.)

#7, p.67. If n is odd, then $n^2 \equiv 1 (mod\, 8)$ and $n^2 \equiv 1 (mod\, 4)$.

$n \pmod 8$	$n^2 \pmod 8$
1	1
3	$9 \equiv 1$
5	$25 \equiv 1$
7	$49 \equiv 1$

If $n^2 \equiv 1 \pmod 8$, then $n^2 \equiv 1 \pmod 4$ for odd n.

MH3.1.1. If $a \equiv b \equiv 1\,(mod\,2)$, show that $a^2 + b^2$ is not a square.

We have the following table:

$n \pmod 4$	$n^2 \pmod 4$
0	0
1	1
2	0
3	1

$a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$. Therefore since $a^2 + b^2 \equiv 2 \pmod 4$,

$a^2 + b^2$ can't be a perfect square.

MH3.1.2 Show that $6|n(n+1)(2n+1)$ for any positive integer n.

$n \pmod 2$	$n(n+1) \pmod 2$
0	0
1	$1(2) \equiv 0$

Therefore $n(n+1)$ is always even.

$n \pmod 3$	$n(n+1)(2n+1) \pmod 3$
0	0
1	$1(2)(3) \equiv 0$
2	$2(3)(5) \equiv 0$

Therefore $n(n+1)(2n+1)$ is always divisible by 3.

Therefore $n(n+1)(2n+1)$ is always divisible by 6.

MH3.1.3 Show that the product of 4 consecutive positive integers is divisible by 24.

$n \pmod 8$	$n(n+1)(n+2)(n+3) \pmod 8$
0	0
1	$1 \cdot 2 \cdot 3 \cdot 4 \equiv 0$
2	$2 \cdot 3 \cdot 4 \cdot 5 \equiv 0$
3	$3 \cdot 4 \cdot 5 \cdot 6 \equiv 360 \equiv 0$
4	$4 \cdot 5 \cdot 6 \cdot 7 \equiv 840 \equiv 0$
5	$5 \cdot 6 \cdot 7 \cdot 8 \equiv 0$
6	$6 \cdot 7 \cdot 8 \cdot 9 \equiv 0$
7	$7 \cdot 8 \cdot 9 \cdot 10 \equiv 0$

Proposition 3.1.7:

(a) If $a \equiv b\,(mod\,m)$ and $d|m$, then $a \equiv b\,(mod\,d)$.

(b) If $ac \equiv bc\,(mod\,m)$, then $a \equiv b\,(mod\,m/(c,m))$.

(c) If $ac \equiv bc\,(mod\,m)$, and if $(c,m) = 1$, then $a \equiv b\,(mod\,m)$.

Proof. (a) is clear.

(b) Let $d = (c,m)$. Then $c = dc'$ and $m = dm'$ where $(c',m') = 1$. Thus $adc' \equiv bdc'\,(mod\,dm')$. Thus $dm'|adc' - bdc'$. Hence $m'|ac' - bc' = (a-b)c'$. Since $(c',m') = 1$, it follows that $m'|(a-b)$. Since $m' = m/d = m/(m,c)$, we get $a \equiv b\,(mod\,m/(c,m))$.

(c) follows from (b). ■

Example: $15 \equiv 45\,(mod\,10)$ so $3(5) \equiv 9(5)\,(mod\,10)$.
However $3 \not\equiv 9\,(mod\,10)$. The best we can say is $3 \equiv 9\,(mod\,\dfrac{10}{(10,5)})$ or $3 \equiv 9\,(mod\,2)$.

Propostion 3.1.10 If $(m,n) = 1$, then $a \equiv b\,(mod\,m)$ and $a \equiv b\,(mod\,n)$ iff $a \equiv b\,(mod\,mn)$

Proof. $a \equiv b\,(mod\,m)$ and $a \equiv b\,(mod\,n)$ iff $m|(a-b)$ and $n|(a-b)$ iff $mn|(a-b)$ iff $a \equiv b\,(mod\,mn)$. ■

Proposition 3.1.3: (Repeat)

(a) $a \equiv a\,mod\,m$

(b) $a \equiv b\,mod\,m$ iff $b \equiv a\,mod\,m$.

(c) $a \equiv b\,mod\,m$ and $b \equiv c\,mod\,m$ imply $a \equiv c\,mod\,m$.

So congruence is an equivalence relation and divides the integers into equivalence classes.

Note: $a \equiv b\,mod\,m$ iff a and b give the same remainder when divided by m.

Example

List the set S_0 of integers $\equiv 0\,mod\,7$.

Solution: $S_0 = \{\ldots, -7, 0, 7, 14, 21, 28, \ldots\}$.

List the set S_1 of integers $\equiv 1\,mod\,7$.

Solution: $S_1 = \{\ldots, -6, 1, 8, 15, 22, \ldots\}$.

List the set S_2 of integers $\equiv 2\,mod\,7$.

Solution: $S_2 = \{\ldots, -5, 2, 9, 16, 23, \ldots\}$.

There are 7 such classes $S_0, \ldots, S_6$. These are denoted $\mathbb{Z}/7\mathbb{Z}$.

Definition 3.1.14 A *complete residue system* modulo m is a set S of integers which contains exactly one member of each equivalence class, i.e. exactly one value congruent to each of $\{0, 1, 2, \ldots, m-1\}$.

Example $\{0, 1, 2, 3, 4\}$ is a complete residue system mod 5. Also $\{0, 6, 12, 3, 9\}$ is a complete residue system mod 5.

EXERCISES p. 67

3.1.1, 2ac, 4, 5, 9, 11,14, 17cd, 20.

Exercise p. 67 # 1) Determine if the following assertions are true:

a) $-2 \equiv 31 \pmod{11}$.

$-2 \equiv 31 \pmod{11} \iff 0 \equiv 33 \pmod{11} \iff 11|33$ which is true.

b) $77 \equiv 5 \pmod{12}$

$77 \equiv 5 \pmod{12} \iff 72 \equiv 0 \pmod{12} \iff 12|72$ which is true,

c) $1111 \equiv 11 \pmod{111}$

$1111 \equiv 11 \pmod{111} \iff 1100 \equiv 0 \pmod{111} \iff 111|1100$ which is false. Therefore $1111 \not\equiv 11 \pmod{111}$.

Exercise p. 67 #2) Compute: a) $2^{83} \pmod{17}$.

$2^4 \equiv 16 \equiv -1 \pmod{17}$, so $2^8 \equiv 1 \pmod{17}$.

$2^{83} \equiv (2^8)^{10} 2^3 \equiv 1^{10} \cdot 8 \equiv 8 \pmod{17}$.

c) $9^{99} \pmod{100}$

Note: **Useful technique:** We can use the binary decomposition of 99 to compute 9^{99} quickly instead of multiplying and reducing 9 99 times.

n	$n \pmod{100}$
9^1	9
9^2	$9 \cdot 9 \equiv 81$
9^4	$81 \cdot 81 \equiv 6561 \equiv 61$
9^8	$61 \cdot 61 \equiv 3721 \equiv 21$
9^{16}	$21 \cdot 21 \equiv 441 \equiv 41$
9^{32}	$41 \cdot 41 \equiv 1681 \equiv 81$
9^{64}	$81 \cdot 81 \equiv 61$

We use the binary representation of 99.

$9^{99} \equiv 9^{64+32+2+1} \equiv 61 \cdot 81 \cdot 81 \cdot 9 \equiv 89 \pmod{100}$.

Exercise p. 67 # 4) Find complete residue systems modulo 11 using only even numbers or only odd numbers.

$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$

Why? If $gcd(a, m) = 1$, then $0, a, 2a, \cdots, (m-1)a$ form a complete residue system modulo m. The m numbers are distinct modulo m since $ai \equiv aj \pmod{m} \Rightarrow m|a(i-j) \Rightarrow m|(i-j) \Rightarrow i = j$.

Odd numbers: $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21\}$ Just add 1 from each number of the complete residue system of even numbers.

Exercise p. 67 # 5) Prove or disprove:

$$a \equiv b \pmod{m} \Rightarrow a^2 \equiv b^2 \pmod{m^2}.$$

Counterexample: $1 \equiv 4 \pmod{3}$ but $1^2 \equiv 1 \not\equiv 16 \equiv 7 \pmod{9}$.

Exercise p. 67 # 9) Show that $3^{2n+5} + 2^{4n+1}$ is divisible by 7 for every integer $n \geq 1$.

$$\begin{aligned}
3^{2n+5} + 2^{4n+1} &\equiv (3^2)^n \times 3^5 + (16)^n \times 2 \pmod{7} \\
&\equiv 2^n \times 243 + 2^n \times 2 \pmod{7} \\
&\equiv 2^n \times 5 + 2^n \times 2 \equiv 2^n(5+2) \equiv 0 \pmod{7}
\end{aligned}$$

Therefore $3^{2n+5} + 2^{4n+1}$ is divisible by 7 for every integer $n \geq 1$.

Exercise p. 67 # 11) Is the sum of three consecutive cubes always divisible by 9?

$n \pmod 9$	$n^3 + (n+1)^3 + (n+2)^3 \pmod 9$
0	$0 + 1 + 8 \equiv 0$
1	$1 + 8 + 27 \equiv 0$
2	$8 + 27 + 64 \equiv 0$
3	$27 + 64 + 125 \equiv 0$
4	$64 + 125 + 216 \equiv 0$
5	$(-4)^3 + (-3)^3 + (-2)^3 \equiv 0$
6	$(-3)^3 + (-2)^3 + (-1)^3 \equiv 0$
7	$(-2)^3 + (-1)^3 + 0^3 \equiv 0$
8	$(-1)^3 + 0^3 + 1^3 \equiv 0$

Therefore the sum of three consecutive cubes is always divisible by 9.

Exercise p. 68 # 17) Let $n = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal representation of n.

a) Prove that n is divisible by 2^k if and only if the number formed by the last k digits is divisible by 2^k.

$$\begin{aligned}
n &\equiv 10^k(a_m 10^{m-k} + a_{m-1}10^{m-1-k} + \cdots + a_k) + a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \cdots + 10a_1 \\
&\quad + a_0 \pmod{2^k} \\
&\equiv 2^k \times 5^k(a_m 10^{m-k} + a_{m-1}10^{m-1-k} + \cdots + a_k) \\
&\quad + a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \cdots + 10a_1 + a_0 \pmod{2^k} \\
&\equiv a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \cdots + 10a_1 + a_0 \pmod{2^k}
\end{aligned}$$

c) Show that n is divisible by 11 if and only if

$$a_0 + a_2 + a_4 + \cdots \equiv a_1 + a_3 + a_5 + \cdots \pmod{11}.$$

We use the fact that $10 \equiv -1 \pmod{11}$.

$$\begin{aligned} n \equiv 0 \pmod{11} \quad &\iff \quad a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \equiv 0 \pmod{11} \\ &\iff \quad a_m(-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_1(-1) + a_0 \equiv 0 \pmod{11} \\ &\iff \quad a_0 + a_2 + a_4 + \cdots \equiv a_1 + a_3 + a_5 + \cdots \pmod{11}. \end{aligned}$$

3.2 Inverses mod m

Definition 3.2.1. A number a' is an *inverse of* a mod m if $aa' \equiv a'a \equiv 1 \mod m$. If a has an inverse, then we say that a is *invertible* mod m.

Examples

An inverse of 2 mod 7 is 4 since $2(4) \equiv 1$ mod 7.

There is no inverse of 4 mod 6 since multiples of 4 mod 6 by 0,1,2,3,4,5 are $0, 4, 2, 0, 4, 2$, mod 6.

The inverse of 5 mod 6 is 5 mod 6 since $5^2 \equiv 1 \, mod \, 6$.

Proposition 3.2.3

(a) An integer a is invertible mod m iff $(a, m) = 1$.

(b) If a has an inverse, then it is unique mod m.

Proof. (a) If $(a, m) = 1$, there exist integers u, v such that $au + mv = 1$. Thus $au \equiv 1 \, mod \, m$ so a is invertible.

Conversely, if a is invertible, then $aa' \equiv 1 \, mod \, m$. Thus $aa' - 1$ is divisible by m so $mk = aa' - 1$. Thus any divisor of a and m must divide 1. Hence $(a, m) = 1$.

(b) Suppose $(a, m) = 1$ and a has two inverses b and b'. Then $ab \equiv ab' \, mod \, m$. So m divides $ab - ab' = a(b - b')$. But $(a, m) = 1$ so $m|(b - b')$ and thus $b \equiv b' \, mod \, m$. ■

Note: The proof above indicates that we can use the Euclidean algorithm to find an inverse mod m.

Example: Find the inverse of 11 modulo 31.

$$\begin{aligned} 31 &= 11(2) + 9 \\ 11 &= 9(1) + 2 \\ 9 &= 2(4) + 1 \\ 2 &= 1(2) \end{aligned}$$

$$\begin{aligned} 1 &= 9 - 2(4) \\ &= 9 - (11 - 9(1))(4) = (-4)11 + (5)9 \\ &= (-4)11 + (5)(31 - 11(2)) = (5)31 - (14)11 \end{aligned}$$

so $1 = (5)31 - (14)11$. Thus $(-14)11 \equiv 1 \pmod{31}$ so -14 is an inverse of 11 modulo 31.

Corollary If a has an inverse a' mod m, then the linear congruence $ax \equiv b$ mod m has a solution for all b.

Proof. $a'a \equiv 1$ mod m. So $ax \equiv b$ mod m implies $a'ax \equiv a'b$ mod m so $x \equiv a'b$ mod m, and this gives the solution. ■

Corollary: If p is prime, then a has an inverse mod p for all $a \not\equiv 0$ mod p.

Note: The integers mod p form a finite field.

Example: Solve $5x \equiv 12$ mod 17.

SOLUTION: Since 17 is prime, 5 has an inverse mod 17.

$$\begin{aligned} 17 &= 5 \times 3 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - (17 - 5 \times 3) \times 2 = -2 \times 17 + 7 \times 5 \end{aligned}$$

Therefore $7 \times 5 \equiv 1 \pmod{17}$, therefore 7 is the inverse of 5 modulo 17. Hence

$5x \equiv 12$ mod 17 implies $7(5)x \equiv 7(12)$ mod 17 or $x \equiv 84$ mod 17 or $x \equiv 16$ mod 17.

Proposition 3.2.7

(a) The linear congruence $ax \equiv b$ mod m has exactly $d = (a, m)$ solutions if $d|b$ and no solutions if $d \nmid b$.

(b) If $ax_0 \equiv b$ mod m for some x_0 then the other distinct solutions mod m are $x_0 + (m/d)i$ for $i = 0, 1, \ldots, d - 1$.

Omit proof.

Example Solve $4x \equiv 6 \, mod \, 10$.

SOLUTION: $(4, 10) = 2 = d$. Since $d|6$, there are exactly $d = 2$ distinct solutions. Look at multiples of 4. They are 4(1)=4,4(2)=8, $4(3) = 12 \equiv 2 \, mod \, 10$, $4(4) = 16 \equiv 6 \, mod \, 10$. Thus $x_0 = 4$. The other solution is $x_0 + (m/d)1 = 4 + (10/2)(1) \equiv 9 \, mod \, 10$.

Wilson's Theorem

If p is prime then $(p-1)! \equiv -1 mod\, p$.

Proof. We try to pair every number in $\{1, 2, \ldots, p-2, p-1\}$ with its inverse mod p. Clearly $1^2 \equiv 1\ mod\, p$ and $(p-1)^2 \equiv 1\, mod\, p$ so 1 pairs with 1 and $(p-1)$ pairs with $p-1$.

Next consider values n such that $2 \leq n \leq p-2$. If $n^2 \equiv 1\, mod\, p$ then $n^2-1 = (n-1)(n+1)$ is divisible by p. So $p|n-1$ or $p|n+1$. But this is impossible since $2 \leq n \leq p-2$. So each of these values pairs with a distinct other value. Hence $(p-1)! \equiv 1(1)\ldots(1)(p-1) \equiv -1\, mod\, p$.

■

Exercises p. 72. #1, 2, 4 ,5, 7, 8

Exercise p. 72 # 1) Determine the invertible elements modulo 15, 17, and 32.

$\{0 \leq a \leq 14 | gcd(a, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ are the invertible elements modulo 15.

17 is prime, so the invertible elements modulo 17 are $\{a | 1 \leq a \leq 16\}$.

$\{0 \leq a \leq 31 | gcd(a, 32) = 1\} = \{1, 3, 5, 7, \ldots, 31\}$.

Exercise p. 72 # 2) Determine the inverse of 67 modulo 119.

We use the Euclidean algorithm.

$$\begin{aligned} 119 &= 67(1) + 52 \\ 67 &= 52(1) + 15 \\ 52 &= 15(3) + 7 \\ 15 &= 7(2) + 1 \\ 7 &= 1(7) \end{aligned}$$

$$\begin{aligned}
1 &= 15 - 7(2)\\
&= 15 - (2)(52 - 15(3)) = -(2)52 + (7)15\\
&= -(2)52 + (7)(67 - 52(1)) = (7)67 - (9)52\\
&= (7)67 - (9)(119 - 67(1)) = -(9)119 + (16)67
\end{aligned}$$

$1 = -(9)119 + (16)67$, therefore $(16)(67) \equiv 1 \pmod{119}$ so the inverse of 67 modulo 119 is 16.

Exercise p. 72 # 4) Solve the following linear congruences.

a) $11x \equiv 28 \pmod{37}$.

11 and 37 are prime, so $(11, 37) = 1$. Therefore there is one solution modulo 37.

We use the Euclidean algorithm to find 11^{-1} modulo 37. Then $x = 11^{-1} \times 28$.

$$\begin{aligned}
37 &= 11(3) + 4\\
11 &= 4(2) + 3\\
4 &= 3(1) + 1\\
3 &= 1(3)
\end{aligned}$$

$$\begin{aligned}
1 &= 4 - (1)3\\
&= 4 - (1)(11 - 4(2)) = -(1)11 + (3)4\\
&= -(1)11 + (3)(37 - 11(3)) = (3)37 - (10)11
\end{aligned}$$

$1 = (3)37 - (10)11$, therefore $(-10)(11) \equiv 1 \pmod{37}$. Therefore $-10 \equiv 27 \pmod{37}$ is the inverse of 11 modulo 37. Therefore $x \equiv 27 \times 28 \equiv 16 \pmod{37}$.

b) $42x \equiv 90 \pmod{156}$.

$gcd(42, 156) = gcd(2 \cdot 3 \cdot 7, 2^2 \cdot 3 \cdot 13) = 6$ and $6|90$. Therefore there are 6 solutions modulo 156.

We use the Euclidean algorithm to find a such that $42a \equiv 6 \pmod{156}$. Then $42(15a) \equiv 90 \pmod{156}$. Then the solutions are $x = 15a + 156/6i$ for $i = 0, 1, \ldots, 5$.

Euclidean algorithm:

$$\begin{aligned} 156 &= 42(3) + 30 \\ 42 &= 30(1) + 12 \\ 30 &= 12(2) + 6 \\ 12 &= 6(2) \end{aligned}$$

$$\begin{aligned} 6 &= 30 - 12(2) \\ &= 30 - (2)(42 - 30(1)) = -(2)42 + (3)30 \\ &= -(2)42 + (3)(156 - 42(3)) = (3)156 - 11(42) \end{aligned}$$

$6 = (3)156 - 11(42)$, so $6 \equiv (-11)42 \pmod{156}$.

$15(-11) \equiv 147 \pmod{156}$. Thus the solutions are: $147, 147 + 26, 147 + 52, 147 + 78, 147 + 104, 147 + 130 \equiv 147, 17, 43, 69, 95, 121 \pmod{156}$.

Exercise p. 72 # 5) Prove that if a^{-1} is the inverse of a modulo m and b^{-1} is the inverse of b modulo m, then $a^{-1}b^{-1}$ is the inverse of ab modulo m.

$ab(a^{-1}b^{-1}) \equiv aa^{-1}bb^{-1} \equiv 1 \cdot 1 \equiv 1 \pmod{m}$. Therefore $a^{-1}b^{-1}$ is the inverse of ab modulo m.

Exercise p. 72 # 7) If m is composite, what is the value $(m-1)!$ (mod m) in the standard residue system? Conclude that $(m-1)! \equiv -1 \pmod{m}$ implies that m is prime.

If m is composite, then m may be factored as $m = d \cdot \frac{m}{d}$ where d and $\frac{m}{d}$ are integers between 2 and $m-1$. Then d and $\frac{m}{d}$ are terms in the product $(m-1)!$ so $(m-1)! \equiv 0 \pmod{m}$. Thus $(m-1)! \equiv -1 \pmod{m}$ implies that m is prime.

Exercise p. 72 # 8)

a) Determine $65! \pmod{67}$.

Note that 67 is prime. By Wilson's Theorem, $66! \equiv -1 \pmod{67}$. $66 \equiv -1 \pmod{67}$ and $66! = 66 \cdot (65!)$. Therefore $65! \equiv 1 \pmod{67}$.

b) If p is a prime number, what is $(p-2)! \pmod{p}$?

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Also, $p-1 \equiv -1 \pmod{p}$. $(p-1)! = (p-1) \cdot ((p-2)!)$. Therefore $(p-2)! \equiv 1 \pmod{p}$.

3.3 CHINESE REMAINDER THEOREM:

CHINESE REMAINDER THEOREM p. 75

Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime. Then

$$
\begin{aligned}
x &\equiv a_1 \, (mod\, m_1) \\
x &\equiv a_2 \, (mod\, m_2) \\
&\cdots \\
x &\equiv a_r \, (mod\, m_r) \qquad (*)
\end{aligned}
$$

has a unique solution mod $(m_1 \cdots m_r)$.

Proof. Let $M = m_1 \cdots m_r$. Let $M_i = M/m_i$ for $i = 1, \ldots, r$.

Because the m_i are pairwise relatively prime, we have $(M_i, m_i) = 1$.
Thus $M_i x \equiv 1\,(mod\, m_i)$ has a solution. Call it x_i.
Let $x \equiv a_1 M_1 x_1 + \cdots + a_r M_r x_r\,(mod\, M)$.
This will be a solution to (*) because

$$a_1 M_1 x_1 + \cdots + a_r M_r x_r \equiv 0 + \cdots + a_i M_i x_i + 0 + \ldots\,(mod\, m_i)$$
$$\equiv a_i(1) \equiv a_i(mod\, m_i).$$

Next assume that there are two solutions x and y mod M. Then $x \equiv y\,(mod\, m_i)\ \forall i$, i.e. $m_i|(x-y)$. Since the m_i are pairwise relatively prime, we have $m_1 \cdots m_r|(x-y)$ or $x \equiv y\,(mod\, m_1 \cdots m_r)$.
■

EXAMPLE Solve the following system of equations.

$$x \equiv 2\,(mod\, 3)$$
$$x \equiv 1\,(mod\, 5)$$
$$x \equiv 6\,(mod\, 8).$$

SOLUTION: $M = 3(5)(8) = 120$. Also 3,5,8 are pairwise relatively prime.
First find M_1, M_2, M_3. These are $5(8), 3(8), 3(5)$ or $40, 24, 15$.
Next solve $M_i x \equiv 1\,(mod\, m_i)$. i.e.

$$40x_1 \equiv 1\,(mod\, 3)$$
$$24x_2 \equiv 1\,(mod\, 5)$$
$$15x_3 \equiv 1\,(mod\, 8).$$

These reduce to

$$1x_1 \equiv 1\,(mod\,3)$$
$$4x_2 \equiv -x_2 \equiv 1\,(mod\,5)$$
$$7x_3 \equiv -x_3 \equiv 1\,(mod\,8).$$

We find $x_1 \equiv 1$ (mod 3), $x_2 \equiv 4$ (mod 5), $x_3 \equiv 7$ (mod 8). Next compute

$$\begin{aligned}&a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3\\&\equiv 2(40)(1) + 1(24)(4) + 6(15)(7) \equiv 80 + 96 + 630\,mod\,120\\&\equiv 806 \equiv 86\,mod\,120\end{aligned}$$

It is easy to check that 86 satisfies the 3 equations in (*).

EXAMPLE Solve

$$x \equiv 4\,mod\,9$$
$$x \equiv 6\,mod\,12$$

SOLUTION: Here 9 and 12 are not relatively prime. So the Chinese Remainder theorem does not work. Note that $x \equiv 6$ mod 12 means $x \equiv 6$ mod 4 and $x \equiv 6$ mod 3. Now we have $x \equiv 4$ mod 9 and $x \equiv 6$ mod 3 so $x \equiv 1$ mod 3 and $x \equiv 0$ mod 3. This is impossible so there is no solution.

EXAMPLE Solve

$$x \equiv 4 \, mod \, 9$$

$$x \equiv 7 \, mod \, 12$$

SOLUTION: The Chinese Reminder Theorem does not apply, since $(9, 12) \neq 1$. Note that $x \equiv 7$ mod 12 means $x \equiv 7 \equiv 3$ mod 4 and $x \equiv 7 \equiv 1$ mod 3. Since $x \equiv 1 \equiv 4$ mod 3 and $x \equiv 4$ mod 9, the intersection of these two sets is $x \equiv 4$ mod 9.

Now we can apply the Chinese remainder theorem to

$$x \equiv 4 \, mod \, 9$$

$$x \equiv 3 \, mod \, 4$$

Take $M = 9(4) = 36$, $M_1 = 4$, $M_2 = 9$.

Solve $M_1 x_1 \equiv 1 \, mod \, m_1$ and $M_2 x_2 \equiv 1 \, mod \, m_2$ or $4x_1 \equiv 1 \, mod \, 9$ and $9x_2 \equiv 1 \, mod \, 4$. We solve these by trying each possible value to get $x_1 \equiv 7 \pmod 9$ and $x_2 \equiv 1 \pmod 4$. (Recall for large numbers, you can use the Euclidean algorithm.) Finally compute

$$a_1 M_1 x_1 + a_2 M_2 x_2 \equiv 4(4)(7) + 3(9)(1) \equiv 112 + 27 \equiv 139 \equiv \ 31 mod \, 36.$$

Exercise(Niven and Zuckerman) Find all integers that give remainders 1,2,3 when divided by 3,4,5.

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

$M_1 = 20$, $M_2 = 15$, and $M_3 = 12$.

$$\begin{aligned} 20x_1 &\equiv 1 \pmod 3 \iff 2x_1 \equiv 1 \pmod 3 \Rightarrow x_1 \equiv 2 \pmod 3 \\ 15x_2 &\equiv 1 \pmod 4 \iff 3x_2 \equiv 1 \pmod 4 \Rightarrow x_2 \equiv 3 \pmod 4 \\ 12x_3 &\equiv 1 \pmod 5 \iff 2x_3 \equiv 1 \pmod 5 \Rightarrow x_3 \equiv 3 \pmod 5 \end{aligned}$$

$x \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 \equiv 1\cdot 20\cdot 2 + 2\cdot 15\cdot 3 + 3\cdot 12\cdot 3 \equiv 238 \equiv 58 \pmod{60}$.
All integers of the form $58 + 60k$ give remainders $1, 2, 3$ when divided by $3, 4, 5$.
The following theorem generalizes the Chinese Remainder Theorem.

Theorem 3.3.4: Let $m_1, \ldots, m_r$ be integers. Then the system of congruences $x \equiv a_i \, mod \, m_i$ $(i = 1, \ldots, r)$ has a solution iff $(m_i, m_j) | a_i - a_j$. The solution is unique mod $lcm[m_1, \ldots, m_r]$.
Proof: See text p. 78.

EXAMPLE The system

$$x \equiv 4\, mod\, 9$$
$$x \equiv 7\, mod\, 12$$

has a unique solution (mod $3^2 2^2$) because $(9,12)|(7-4)$.

Exercises: p. 80 #1ab, 2ab, 4, 5,

Exercise p. 80 # 1)

a)

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

$M_1 = 105,\ M_2 = 70,\ M_3 = 42,\ M_4 = 30.$

$$\begin{aligned} M_1 x_1 &\equiv 1 \pmod{m_1} \iff 105x_1 \equiv 1 \pmod 2 \iff x_1 \equiv 1 \pmod 2 \\ M_2 x_2 &\equiv 1 \pmod{m_2} \iff 70x_2 \equiv 1 \pmod 3 \iff x_2 \equiv 1 \pmod 3 \\ M_3 x_3 &\equiv 1 \pmod{m_3} \iff 42x_3 \equiv 1 \pmod 5 \iff 2x_3 \equiv 1 \pmod 5 \\ &\iff x_3 \equiv 3 \pmod 5 \\ M_4 x_4 &\equiv 1 \pmod{m_4} \iff 30x_4 \equiv 1 \pmod 7 \iff 2x_4 \equiv 1 \pmod 7 \\ &\iff x_4 \equiv 4 \pmod 7 \end{aligned}$$

$$
\begin{aligned}
x &\equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \\
&\equiv 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 4 \cdot 42 \cdot 3 + 2 \cdot 30 \cdot 4 \equiv 989 \equiv 149 \pmod{210}
\end{aligned}
$$

so $x \equiv 149 \pmod{210}$.

Exercise p. 80 # 2) Determine if the following simultaneous congruences have a solution, and find the smallest positive solution if it exists.

a)

$$
\begin{aligned}
x &\equiv 3 \pmod{8} \\
x &\equiv 7 \pmod{12} \\
x &\equiv 4 \pmod{15}
\end{aligned}
$$

$4 = (8,12)|(3-7)$

$3 = (12,15)|(7-4)$

$1 = (8,15)|(3-4)$

Therefore the system has a solution that is unique modulo $lcm(8,12,15) = lcm(2^3, 2^2 \cdot 3, 3 \cdot 5) = 2^3 \cdot 3 \cdot 5 = 120$.

We look at prime powers:

$$
\begin{aligned}
x &\equiv 3 \pmod 8 & (1)\\
x &\equiv 7 \pmod 4 & (2)\\
x &\equiv 7 \pmod 3 & (3)\\
x &\equiv 4 \pmod 3 & (4)\\
x &\equiv 4 \pmod 5 & (5)
\end{aligned}
$$

(1) implies (2) and (3) and (4) are equivalent. Thus we are reduced to solving the system:

$$
\begin{aligned}
x &\equiv 3 \pmod 8\\
x &\equiv 1 \pmod 3\\
x &\equiv 4 \pmod 5
\end{aligned}
$$

$M_1 = 15,\ M_2 = 40,\ M_3 = 24$

$$
\begin{aligned}
M_1x_1 &\equiv 1 \pmod{m_1} \iff 15x_1 \equiv 1 \pmod 8 \iff -x_1 \equiv 1 \pmod 8\\
&\iff x_1 \equiv 7 \pmod 8\\
M_2x_2 &\equiv 1 \pmod{m_2} \iff 40x_2 \equiv 1 \pmod 3 \iff x_2 \equiv 1 \pmod 3\\
M_3x_3 &\equiv 1 \pmod{m_3} \iff 24x_3 \equiv 1 \pmod 5 \iff -x_2 \equiv 1 \pmod 5\\
&\iff x_2 \equiv 4 \pmod 5
\end{aligned}
$$

$$
\begin{aligned}
x &\equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3\\
&\equiv 3 \cdot 15 \cdot 7 + 1 \cdot 40 \cdot 1 + 4 \cdot 24 \cdot 4 \equiv 739 \equiv 19 \pmod{120}
\end{aligned}
$$

The smallest positive solution is $x = 19$.

b)

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 8 \pmod{12} \\ x &\equiv 12 \pmod{18} \end{aligned}$$

$(6, 12) = 6 \nmid (12 - 4) = 8$, so there is no solution.

3.4 POLYNOMIAL CONGRUENCES p.81

Example: $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{503}$ is an example of a polynomial congruence of degree greater than 1.

A solution or root of a polynomial congruence $f(x) \equiv 0 \pmod{m}$ is an integer r such that $f(r) \equiv 0 \pmod{m}$.

The roots r are to be considered mod m.

Example A solution of $x^2 + 2x \equiv 4$ mod 5 is $r \equiv 4$ mod 5.

Note: Let $m = p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of m. Then $f(x) \equiv 0$ mod m is equivalent to $f(x) \equiv 0$ mod $p_1^{a_i}$ for all $i = 1, \ldots, k$. These systems can be solved with the help of the Chinese Remainder Theorem.

Example: Solve $x^2 \equiv 4$ mod 117.

SOLUTION: $117 = 3^2 13^1$. So we solve $x^2 \equiv 4$ mod 9 and $x^2 \equiv 4$ mod 13. We can solve these by listing all cases 0,1,2,3,4,5,6,7,8 mod 9 and 0,1,2,3,4,5, 6, 7, 8,9,10,11,12 mod 13. The solutions are

$r \equiv 2, 7$ mod 9 and $r \equiv 2, 11$ mod 13. This gives 4 pairs

$$r \equiv 2 mod\, 9 \quad r \equiv 2 mod\, 9 \qquad\qquad r \equiv 7 mod\, 9 \quad r \equiv 7 mod\, 9$$
$$r \equiv 2 mod\, 13 \quad r \equiv 11\, mod 13 \qquad\qquad r \equiv 2 mod\, 13 \quad r \equiv 11 mod\, 13$$

The solution to the first pair is clearly $r \equiv 2$ mod 9(13).

The solutions to the other pairs require the Chinese remainder theorem.

$r \equiv 2$ mod 9 and $r \equiv 11$ mod 13 give $r \equiv a_1M_1x_1 + a_2M_2x_2 \equiv 2(13)x_1 + 11(9)x_2$ mod 117 where $13x_1 \equiv 1(mod\, 9)$ and $9x_2 \equiv 1(mod\, 13)$. We find $x_1 \equiv 7$ mod 9 and $x_2 \equiv 3$ mod 13, by trying all possiblities (or you can use the Euclidean algorithm).

So our solution is $r \equiv 2(13)(7) + 11(9)(3) \equiv 182 + 297 \equiv 479 \equiv 11$ mod 117.

The other two cases give $r \equiv 106$ and $r \equiv 115$ mod 117.

So the four solutions are $r \equiv 2, 11, 106, 115$ mod 117.

Reduction in Exponent Technique.

Example Solve (*) $x^2 + 3x \equiv 19$ mod 49(=7^2).

SOLUTION:

$x^2 + 3x \equiv 19$ mod 49(=7^2) $\Rightarrow x^2 + 3x \equiv 19$ mod 7

so $x^2 + 3x \equiv 5$ mod 7. Try $x \equiv 0, 1, 2, 3, 4, 5, 6$ mod 7. The solutions are 5,6 mod 7.

So $x \equiv 7a + 5$ mod 49 or $x \equiv 7b + 6$ mod 49.

CASE 1: $x \equiv 7a + 5$ mod 49. Then (*) gives

$19 \equiv x^2 + 3x \equiv (7a + 5)^2 + 3(7a + 5) = 49a^2 + 70a + 25 + 21a + 15$ mod 49. So

$91a+21 \equiv 0 \bmod 49$ so $7(13a+3) \equiv 0 \bmod 49$ so $13a+3 \equiv 0 \bmod 7$ so $6a+3 \equiv 0 \bmod 7$

so $2a+1 \equiv 0 \bmod 7$. Try $a \equiv 0,1,2,3,4,5,6 \bmod 7$. The solution is $a \equiv 3 \bmod 7$.

So $a = 7c+3$. Then $x \equiv 7a+5 \equiv 7(7c+3)+5 \equiv 49c+26 \equiv 26 \bmod 49$.

CASE 2: $x \equiv 7b+6 \bmod 49$. Then (*) gives

$19 \equiv x^2+3x \equiv (7b+6)^2+3(7b+6) = 49b^2+84b+36+21b+18 \bmod 49$. So

$105b+35 \equiv 0 \bmod 49$ so $7(15b+5) \equiv 0 \bmod 49$ so $15b+5 \equiv 0 \bmod 7$ so $3b+1 \equiv 0 \bmod 7$

so $3b+1 \equiv 0 \bmod 7$. Try $b \equiv 0,1,2,3,4,5,6 \bmod 7$. The solution is $b \equiv 2 \bmod 7$.

So $b = 7d+2$. Then $x \equiv 7b+6 \equiv 7(7d+2)+6 \equiv 49d+20 \equiv 20 \bmod 49$.

FINAL SOLUTION: $x \equiv 26$ or $20 \bmod 49$.

Programming in R:

```
> x=1:49
> x
 [1]  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
[20] 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
[39] 39 40 41 42 43 44 45 46 47 48 49
> y=x^2+3*x
> z=y-49*floor(y/49)
> z
```

```
 [1]  4 10 18 28 40  5 21 39 10 32  7 33 12 42 25 10 46 35 26
[20] 19 14 11 10 11 14 19 26 35 46 10 25 42 12 33  7 32 10 39
[39] 21  5 40 28 18 10  4  0 47 47  0
> x[z==19]
[1] 20 26
```

Lemma 3.4.a: If $f(x)$ is a polynomial, then $f(x+y) = f(x) + yf'(x) + y^2 g(x,y)$.

Proof. : By Taylor's theorem,

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f^{(2)}(x_0)}{2!}(x - x_0)^2 + \dots .$$

Replace x by $x + y$ and x_0 by x to get

$$\begin{aligned} f(x+y) &= f(x) + \frac{f'(x)}{1!}y + \frac{f^{(2)}(x)}{2!}y^2 + \dots \\ &= f(x) + \frac{f'(x)}{1!}y + y^2 g(x,y). \end{aligned}$$

■

Lemma 3.4.b: If $f(x)$ is a polynomial with integer coefficients, and p is prime, then

$$f(x_0 + kp) \equiv f(x_0) + kpf'(x_0)(\bmod p^2).$$

Proof: Apply lemma 3.4.a with $x = x_0$ and $y = kp$. □

Property: If x_0 is a solution to $f(x) \equiv 0 \bmod p$, then solutions to

$f(x) \equiv 0 \bmod p^2$ (if they exist) are of the form $x_0 + kp$ where

$$kf'(x_0) \equiv -f(x_0)/p \bmod p.$$

Proof. If $f(x) \equiv 0 \bmod p^2$ then $f(x) \equiv 0 \bmod p$. Since $f(x_0) \equiv 0 \bmod p$ and $f(x_0 + kp) \equiv 0 \bmod p^2$, lemma 3.4.b gives

$$0 \equiv f(x_0 + kp) \equiv f(x_0) + kpf'(x_0)(\bmod p^2).$$

Divide by p to get $0 \equiv f(x_0)/p + kf'(x_0)$. When we solve for k, we have all solutions mod p^2. ■

Example p.85

Find all solutions to $4x^2 + 4x - 3 \equiv 0 \bmod 49$ ($=7^2$).

SOLUTION:

First solve $4x^2 + 4x - 3 \equiv 0 \bmod 7$. Try $x \equiv 0, 1, 2, 3, 4, 5, 6$. The two solutions are $x_0 \equiv 2, 4 \bmod 7$.

Case 1: $x_0 \equiv 2 \bmod 7$. Then a solution to the original polynomial congruence has form $x_0 + k(7)$ where $kf'(x_0) \equiv -f(x_0)/p \bmod p$. But $f'(x_0) = 8x_0 + 4|_{x_0=2} \equiv 20 \pmod{49}$ and $f(x_0) \equiv 4(2^2) + 4(2) - 3 \equiv 21 \bmod 49$. So $kf'(x_0) \equiv -f(x_0)/p \bmod p$, i.e. $20k \equiv -21/7 \bmod 7$ so $6k \equiv -3 \bmod 7$ or $2k \equiv -1 \bmod 7$. Try $k = 0, 1, 2, 3, 4, 5, 6$. We see that $k = 3$ is the only solution. So $x_0 + kp \equiv 2 + 3(7) \equiv 23 \bmod 49$.

Case 2: $x_0 \equiv 4 \bmod 7$. Then a solution to the original polynomial congruence has form $x_0 + k(7)$ where $kf'(x_0) \equiv -f(x_0)/p \bmod p$. But $f'(x_0) = 8x_0 + 4|_{x_0=4} \equiv 36 \pmod{49}$ and $f(x_0) \equiv 4(4^2) + 4(4) - 3 \equiv 77 \equiv 28 \bmod 49$. So $kf'(x_0) \equiv -f(x_0)/p \bmod p$, i.e.

$36k \equiv -28/7 \bmod 7$ so $k \equiv -4 \equiv 3 \bmod 7$. Clearly $k = 3$ is the only solution. So $x_0 + kp \equiv 4 + 3(7) \equiv 25 \bmod 49$.

Check using R

```
> x=1:49
> x
 [1]  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
[20] 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
[39] 39 40 41 42 43 44 45 46 47 48 49
> y=4*x^2 +4*x -3
> z=y-49*floor(y/49)
> z
 [1]  5 21 45 28 19 18 25 40 14 45 35 33 39  4 26  7 45 42 47
[20] 11 32 12  0 45  0 12 32 11 47 42 45  7 26  4 39 33 35 45
[39] 14 40 25 18 19 28 45 21  5 46 46
> x[z==0]
[1] 23 25
```

Theorem 3.4.6 (p. 84)
Let $f(x)$ be a polynomial with integer coefficients and let $f'(x)$ be its derivative. Let x_0 be a solution of $f(x) \equiv 0 \bmod p^k$.
(a) If $p \nmid f'(x_0)$, then there is a unique solution $x \equiv x_0 + p^k t$ to $f(x) \equiv 0 \pmod{p^{k+1}}$, where t is the unique solution to

$$p^k t f'(x_0) \equiv -f(x_0) \pmod{p^{k+1}}.$$

(b) If $p | f'(x_0)$ and $p^{k+1} | f(x_0)$, then $f(x) \equiv 0 \pmod{p^{k+1}}$ has p

incongruent solutions given by $x \equiv x_0 + p^k t \pmod{p^{k+1}}$ for any value of t mod p.
(c) If $p|f'(x_0)$ and $p^{k+1} \nmid f(x_0)$, then there is no solution x to $f(x) \equiv 0 \pmod{p^{k+1}}$ such that $x \equiv x_0 \pmod{p^k}$.
Proof: see text.

Exercises: (p. 86) 1b,1c, 2a, 3, 5, 8.
Exercise p. 86 # 1) Find all solutions to the following equations.
b) $x^2 + 4x + 10 \equiv 0 \pmod{11^2}$.
First solve $x^2 + 4x + 10 \equiv 0 \pmod{11}$.
This has solutions $x_0 \equiv 2 \pmod{11}$ and $x_0 \equiv 5 \pmod{11}$.
Case 1: $x_0 = 2$.
$f'(2) = 2 \cdot 2 + 4 = 8$ and $11 \nmid 8$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{11^2}$.

$$\begin{aligned} tp^k f'(x_0) &\equiv -f(x_0) \pmod{p^{k+1}} \\ 11tf'(2) &\equiv -f(2) \pmod{11^2} \\ 11t \cdot 8 &\equiv -22 \pmod{11^2} \\ 8t &\equiv -2 \equiv 9 \pmod{11} \\ t &\equiv 8 \pmod{11} \end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 2 + 11 \cdot 8 \equiv 90 \pmod{11^2}$ is a solution to $f(x) \equiv 0 \pmod{11^2}$.
Case 2: $x_0 = 5$.
$f'(5) = 2 \cdot 5 + 4 = 14$ and $11 \nmid 14$, so there is a unique solution

$x = x_0 + pt$ to $f(x) \equiv 0 \pmod{11^2}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{p^{k+1}} \\
11tf'(5) &\equiv -f(5) \pmod{11^2} \\
11t \cdot 14 &\equiv -55 \pmod{11^2} \\
14t &\equiv -5 \pmod{11} \\
3t &\equiv 6 \pmod{11} \\
t &\equiv 2 \pmod{11}
\end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 5 + 11 \cdot 2 \equiv 27 \pmod{11^2}$ is a solution to $f(x) \equiv 0 \pmod{11^2}$.

Therefore the solutions are $x \equiv 90 \pmod{11^2}$ and $x \equiv 27 \pmod{11^2}$.

c) $x^3 + 5x^2 + 2x - 1 \equiv 0 \pmod{7^2}$.

First solve $x^3 + 5x^2 + 2x - 1 \equiv 0 \pmod{7}$.

Trying 0 to 6, we see that $x_0 \equiv 1 \pmod{7}$, $x_0 \equiv 3 \pmod{7}$, and $x_0 \equiv 5 \pmod{7}$ are solutions.

Case 1: $x_0 = 1$

$f'(1) = 3 + 10 + 2 = 15$ and $7 \nmid 15$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{7^2}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{7^2} \\
7tf'(1) &\equiv -f(1) \pmod{7^2} \\
7t \cdot 15 &\equiv -7 \pmod{7^2} \\
15t &\equiv -1 \pmod{7} \\
t &\equiv 6 \pmod{7}
\end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 1 + 7 \cdot 6 \equiv 43 \pmod{7^2}$ is a solution to $f(x) \equiv 0 \pmod{7^2}$.

Case 2: $x_0 = 3$

$f'(3) = 3 \cdot 3^2 + 10 \cdot 3 + 2 = 59$ and $7 \nmid 59$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{7^2}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{7^2} \\
7tf'(3) &\equiv -f(3) \pmod{7^2} \\
7t \cdot 59 &\equiv -77 \pmod{7^2} \\
59t &\equiv -11 \pmod{7} \\
3t &\equiv 3 \pmod{7} \\
t &\equiv 1 \pmod{7}
\end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 3 + 7 \cdot 1 = 10 \pmod{7^2}$ is a solution to $f(x) \equiv 0 \pmod{7^2}$.

Case 3: $x_0 = 5$:

$f'(5) = 3 \cdot 5^2 + 10 \cdot 5 + 2 = 127$ and $7 \nmid 127$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{7^2}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{7^2} \\
7tf'(5) &\equiv -f(5) \pmod{7^2} \\
7t \cdot 127 &\equiv -259 \pmod{7^2} \\
127t &\equiv -37 \pmod{7} \\
t &\equiv 5 \pmod{7}
\end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 5 + 7 \cdot 5 = 40 \pmod{7^2}$ is a solution to

$f(x) \equiv 0 \pmod{7^2}$.

Therefore the solutions to $f(x) \equiv 0 \pmod{7^2}$ are $x \equiv 43, 10, 40 \pmod{49}$.

Exercise p. 87 # 2a) Solve $x^2 + 12x - 17 \equiv 0 \pmod{143}$.

This is equivalent to the system

$$\begin{aligned} x^2 + 12x - 17 \equiv 0 \quad (\text{mod } 11) \\ x^2 + 12x - 17 \equiv 0 \quad (\text{mod } 13) \end{aligned}$$

The first equation has solutions $x \equiv 2 \pmod{11}$ and $x \equiv 8 \pmod{11}$.

The second equation has solutions $x \equiv 6 \pmod{13}$ and $x \equiv 8 \pmod{13}$.

Case 1:

$$\begin{aligned} x &\equiv 2 \quad (\text{mod } 11) \\ x &\equiv 6 \quad (\text{mod } 13) \end{aligned}$$

$M_1 = 13,\ M_2 = 11$

$$\begin{aligned} 13x_1 &\equiv 1 \quad (\text{mod } 11) \iff 2x_1 \equiv 1 \quad (\text{mod } 11) \iff x_1 \equiv 6 \quad (\text{mod } 11) \\ 11x_2 &\equiv 1 \quad (\text{mod } 13) \iff -2x_2 \equiv 1 \quad (\text{mod } 13) \iff x_2 \equiv -7 \quad (\text{mod } 13) \\ &\iff x_2 \equiv 6 \quad (\text{mod } 13) \end{aligned}$$

$$\begin{aligned} x &\equiv a_1 M_1 x_1 + a_2 M_2 x_2 \\ &\equiv 2 \cdot 13 \cdot 6 + 6 \cdot 11 \cdot 6 \equiv 552 \equiv 123 \quad (\text{mod } 143) \end{aligned}$$

Case 2:

$$\begin{aligned} x &\equiv 2 \pmod{11} \\ x &\equiv 8 \pmod{13} \end{aligned}$$

$$\begin{aligned} x &\equiv a_1M_1x_1 + a_2M_2x_2 \\ &\equiv 2 \cdot 13 \cdot 6 + 8 \cdot 11 \cdot 6 \equiv 684 \equiv 112 \pmod{143} \end{aligned}$$

Case 3:

$$\begin{aligned} x &\equiv 8 \pmod{11} \\ x &\equiv 6 \pmod{13} \end{aligned}$$

$$\begin{aligned} x &\equiv a_1M_1x_1 + a_2M_2x_2 \\ &\equiv 8 \cdot 13 \cdot 6 + 6 \cdot 11 \cdot 6 \equiv 1020 \equiv 19 \pmod{143} \end{aligned}$$

Case 4:

$$\begin{aligned} x &\equiv 8 \pmod{11} \\ x &\equiv 8 \pmod{13} \end{aligned}$$

Then $x \equiv 8 \pmod{143}$.

Therefore the solutions are: $x \equiv 123, 112, 19, 8 \pmod{143}$.

Exercise p. 87 # 3) Without using a computer, determine all integers x such that the last three digits of x^3 are the same as those of x.

$x^3 \equiv x \pmod{1000} \iff x^3 - x \equiv 0 \pmod{1000}$. This is equivalent to the system of simultaneous equation:

$$\begin{aligned} x^3 - x &\equiv 0 \pmod{8} \\ x^3 - x &\equiv 0 \pmod{125} \end{aligned}$$

$x^3 - x = x(x-1)(x+1)$. Therefore the solutions to the first equation are: $x \equiv 0, 1, 3, 5, 7 \pmod{8}$.

The solutions to the second equation are $x \equiv 0, 1, 124 \pmod{125}$.

We also illustrate how to find the solutions to the second equation using reduction in exponent.

First, solve $x^3 - x \equiv 0 \pmod{5}$. The solutions are $x_0 \equiv 0, 1, 4 \pmod{5}$.

Case 1: $x_0 \equiv 0 \pmod{5}$:

$f'(0) = -1$ and $5 \nmid -1$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{5^2}$.

$$\begin{aligned} tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^2} \\ 5t(-1) &\equiv 0 \pmod{5^2} \\ t &\equiv 0 \pmod{5} \end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 0 \pmod{5^2}$ is a solution to $f(x) \equiv 0 \pmod{5^2}$.

Again, $5 \nmid f'(0)$, so there is a unique solution $x = x_0 + p^2 t$ to $f(x) \equiv 0$

(mod 5^3).

$$\begin{aligned} tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^3} \\ 5^2 t(-1) &\equiv 0 \pmod{5^3} \\ t &\equiv 0 \pmod{5} \end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 0 \pmod{5^3}$ is a solution to $f(x) \equiv 0 \pmod{5^3}$.

Case 2: $x_0 \equiv 1 \pmod{5}$

$f'(1) = 3 - 1 = 2$ and $5 \nmid 2$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{5^2}$.

$$\begin{aligned} tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^2} \\ 5t(2) &\equiv 0 \pmod{5^2} \\ 2t &\equiv 0 \pmod{5} \\ t &\equiv 0 \pmod{5} \end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 1 \pmod{5^2}$ is a solution to $f(x) \equiv 0 \pmod{5^2}$.

Again, $5 \nmid f'(0)$, so there is a unique solution $x = x_0 + p^2 t$ to $f(x) \equiv 0 \pmod{5^3}$.

$$\begin{aligned} tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^3} \\ 5^2 t(2) &\equiv 0 \pmod{5^3} \\ t &\equiv 0 \pmod{5} \end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 1 \pmod{5^3}$ is a solution to $f(x) \equiv 0$

(mod 5^3).

Case 3: $x_0 \equiv 4 \pmod 5$

$f'(4) = 3 \cdot 4^2 - 1 = 47$ and $5 \nmid 47$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{5^2}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^2} \\
5t(47) &\equiv -60 \pmod{5^2} \\
47t &\equiv -12 \pmod 5 \\
2t &\equiv 3 \pmod 5 \\
t &\equiv 4 \pmod 5
\end{aligned}$$

Therefore $x \equiv x_0 + pt \equiv 4 + 20 \equiv 24 \pmod{25}$ is a solution to $f(x) \equiv 0 \pmod{5^2}$.

$f'(24) = 1727$ and $5 \nmid 1727$, so there is a unique solution $x = x_0 + pt$ to $f(x) \equiv 0 \pmod{5^3}$.

$$\begin{aligned}
tp^k f'(x_0) &\equiv -f(x_0) \pmod{5^3} \\
25t(1727) &\equiv -13800 \pmod{5^3} \\
1727t &\equiv -552 \pmod 5 \\
2t &\equiv -2 \pmod 5 \\
t &\equiv -1 \equiv 4 \pmod 5
\end{aligned}$$

Therefore $x \equiv x_0 + p^k t \equiv 24 + 25 \cdot 4 \equiv 124 \pmod{5^3}$ is a solution to $f(x) \equiv 0 \pmod{5^3}$.

Therefore the solutions to $x^3 - x \equiv 0 \pmod{125}$ are $x \equiv 0, 1, 124$ (mod 125).

We now use the Chinese Remainder Theorem to find the solutions modulo 1000.

$M_1 = 125,\ M_2 = 8.$

$$\begin{aligned} 125x_1 &\equiv 1 \pmod 8 \\ 5x_1 &\equiv 1 \pmod 8 \\ x_1 &\equiv 5 \pmod 8 \end{aligned}$$

$$\begin{aligned} 8x_2 &\equiv 1 \pmod{125} \\ x_2 &\equiv 47 \pmod{125} \quad \text{by the Euclidean Algorithm} \end{aligned}$$

a_1	a_2	$x \equiv a_1 M_1 x_1 + a_2 M_2 x_2$
0	0	0
0	1	$0 + 1 \cdot 8 \cdot 47 \equiv 376$
0	124	$0 + 124 \cdot 8 \cdot 47 \equiv 624$
1	0	$1 \cdot 125 \cdot 5 \equiv 625$
1	1	1
1	124	$1 \cdot 125 \cdot 5 + 124 \cdot 8 \cdot 47 \equiv 249$
3	0	$3 \cdot 125 \cdot 5 \equiv 875$
3	1	$3 \cdot 125 \cdot 5 + 1 \cdot 8 \cdot 47 \equiv 251$
3	124	$3 \cdot 125 \cdot 5 + 124 \cdot 8 \cdot 47 \equiv 499$
5	0	$5 \cdot 125 \cdot 5 \equiv 125$
5	1	$5 \cdot 125 \cdot 5 + 1 \cdot 8 \cdot 47 \equiv 501$
5	124	$5 \cdot 125 \cdot 5 + 124 \cdot 8 \cdot 47 \equiv 749$
7	0	$7 \cdot 125 \cdot 5 \equiv 375$
7	1	$7 \cdot 125 \cdot 5 + 1 \cdot 8 \cdot 47 \equiv 751$
7	124	$7 \cdot 125 \cdot 5 + 124 \cdot 8 \cdot 47 \equiv 999$

Therefore the integers x such that the last three digits of x^3 are the same as those of x are those ending in the digits: $000, 376, 624, 625$, 001, 249, 875, 251, 499, $125, 501, 749, 375, 751, 999$.