Applications of Congruences

Section 4.5

Pseudorandom Numbers

- Randomly chosen numbers are needed for many purposes, including computer simulations.
- *Pseudorandom numbers* are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.
- Four integers are needed: the *modulus* m, the *multiplier* a, the *increment* c, and *seed* x_0, with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

(*an example of a recursive definition, discussed in Section* 5.3*)*

- If psudorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n/m.

Pseudorandom Numbers

- **Example**: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.
- **Solution**: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \bmod 9$, with $x_0 = 3$.

  $x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$
  $x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$
  $x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$
  $x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$
  $x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$
  $x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$
  $x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$
  $x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$
  $x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$

  The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...

  It repeats after generating 9 terms.
- Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Cryptography

Section 4.6

Section Summary

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Crytographic Protocols
- Primitive Roots and Discrete Logarithms

Caesar Cipher

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.) For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Here is how the encryption process works:

- Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3) \bmod 26$. It replaces each integer p in the set $\{0,1,2,\ldots,25\}$ by $f(p)$ in the set $\{0,1,2,\ldots,25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example: Encrypt the message "MEET YOU IN THE PARK" using the Caesar cipher.

Solution: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating the numbers back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN."

Caesar Cipher

- To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.
- The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

  $f(p) = (p + k) \bmod 26$

  and the decryption function is

  $f^{-1}(p) = (p-k) \bmod 26$

  The integer k is called a *key*.

Shift Cipher

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11) \bmod 26$, yielding

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating the numbers back to letters produces the ciphertext

"DEZA RWZMLW HLCXTYR."

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Shift each of the numbers by $-k = -7$ modulo 26, yielding

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

Proofs (1.7)

Overview

Proofs: General Techniques

- Direct Proof
- Indirect Proof
- Proof by Contradiction

Proof Nuts and Bolts

A proof is a logically structured argument which demonstrates that a certain proposition is true. When the proof is complete, the resulting proposition becomes a ***theorem***, or if it is rather simple, a ***lemma***.

For example, consider the proposition:

If k is any integer such that $k \equiv 1 \pmod 3$,
then $k^3 \equiv 1 \pmod 9$.

Let's prove this fact:

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

112

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$

113

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$

114

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$

115

Proofs
Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$

116

Proofs
Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$
5. $\exists n\ \ k^3 = 27n^3 + 27n^2 + 9n + 1$

117

Proofs
Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$
5. $\exists n\ \ k^3 = 27n^3 + 27n^2 + 9n\ + 1$
6. $\exists n\ \ k^3-1 = 27n^3 + 27n^2 + 9n$

118

Proofs
Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ \ k-1 = 3n$
3. $\exists n\ \ k = 3n + 1$
4. $\exists n\ \ k^3 = (3n + 1)^3$
5. $\exists n\ \ k^3 = 27n^3 + 27n^2 + 9n\ + 1$
6. $\exists n\ \ k^3-1 = 27n^3 + 27n^2 + 9n$
7. $\exists n\ \ k^3-1 = (3n^3 + 3n^2 + n)\cdot 9$

119

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ k-1 = 3n$
3. $\exists n\ k = 3n + 1$
4. $\exists n\ k^3 = (3n + 1)^3$
5. $\exists n\ k^3 = 27n^3 + 27n^2 + 9n + 1$
6. $\exists n\ k^3-1 = 27n^3 + 27n^2 + 9n$
7. $\exists n\ k^3-1 = (3n^3 + 3n^2 + n)\cdot 9$
8. $\exists m\ k^3-1 = m\cdot 9$

120

Proofs

Example

PROVE: $\forall k \in \mathbf{Z}\ k \equiv 1 \pmod 3 \rightarrow k^3 \equiv 1 \pmod 9$

1. $k \equiv 1 \pmod 3$
2. $\exists n\ k-1 = 3n$
3. $\exists n\ k = 3n + 1$
4. $\exists n\ k^3 = (3n + 1)^3$
5. $\exists n\ k^3 = 27n^3 + 27n^2 + 9n + 1$
6. $\exists n\ k^3-1 = 27n^3 + 27n^2 + 9n$
7. $\exists n\ k^3-1 = (3n^3 + 3n^2 + n)\cdot 9$
8. $\exists m\ k^3-1 = m\cdot 9$
9. $k^3 \equiv 1 \pmod 9$

121

Direct Proofs

Previous was an example of a ***direct proof***. I.e., to prove that a proposition of the form "$\forall k\ P(k) \rightarrow Q(k)$" is true, needed to derive that "$Q(k)$ is true" for any k which satisfied "$P(k)$ is true".

Three basic steps in a direct proof:

122

Direct Proofs

1) **Deconstruct Axioms**

Take the hypothesis and turn it into a usable form.
Usually this amounts to just applying the definition.

EG: $k \equiv 1 \pmod 3$ really means $3|(k-1)$ which actually means
$\exists n \quad k-1 = 3n$

123

Direct Proofs

2) **Mathematical Insights**

Use your human intellect and get at "real reason" behind theorem.

EG: looking at what we're trying to prove, we see that we'd really like to understand k^3. So let's take the cube of k ! From here, we'll have to use some algebra to get the formula into a form usable by the final step:

124

Direct Proofs

3) **Reconstruct Conclusion**

This is the reverse of step 1. At the end of step 2 we should have a simple form that could be derived by applying the definition of the conclusion.

EG. $k^3 \equiv 1 \pmod 9$ is readily gotten from

$\exists m\ k^3 - 1 = m \cdot 9$ since the latter is the definition of the former.

125

Proofs
Indirect

In addition to direct proofs, there are two other standard methods for proving

$$\forall k\, P(k) \rightarrow Q(k)$$

1. ***Indirect Proof***

   For any k assume: $\neg Q(k)$

   and derive: $\neg P(k)$

Uses the contrapositive logical equivalence: $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$

126

Proofs
Reductio Ad Absurdum

2. ***Proof by Contradiction*** (***Reductio Ad Absurdum***)

   For any k assume: $P(k) \wedge \neg Q(k)$

   and derive: $\neg P(k) \vee Q(k)$

Uses the logical equivalence:

$$P \rightarrow Q \Leftrightarrow \neg P \vee Q \Leftrightarrow \neg P \vee Q \vee \neg P \vee Q$$
$$\Leftrightarrow (\neg P \vee Q) \vee (\neg P \vee Q) \Leftrightarrow \neg(P \wedge \neg Q) \vee (\neg P \vee Q)$$
$$\Leftrightarrow (P \wedge \neg Q) \rightarrow (\neg P \vee Q)$$

Intuitively: Assume claim is false (so P must be true and Q false). Show that assumption was absurd (so P false or Q true) so claim true!

127

Indirect Proof Example

PROVE: The square of an even number is even.

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \; k^2 = 2n + 1$
4. $\exists n \; k^2 - 1 = 2n$

132

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \; k^2 = 2n + 1$
4. $\exists n \; k^2 - 1 = 2n$
5. $\exists n \; (k - 1)(k + 1) = 2n$

133

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$

134

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$
7. $2 \mid (k - 1) \;\vee\; 2 \mid (k + 1)$ since 2 is prime

135

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$
7. $2 \mid (k - 1) \;\vee\; 2 \mid (k + 1)$ since 2 is prime
8. $\exists a \;\; k - 1 = 2a \;\vee\; \exists b \;\; k+1 = 2b$

136

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$
7. $2 \mid (k - 1) \;\vee\; 2 \mid (k + 1)$ since 2 is prime
8. $\exists a \;\; k - 1 = 2a \;\vee\; \exists b \;\; k+1 = 2b$
9. $\exists a \;\; k = 2a + 1 \vee \;\exists b \;\; k = 2b - 1$

137

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$
7. $2 \mid (k - 1) \;\vee\; 2 \mid (k + 1)$ since 2 is prime
8. $\exists a \;\; k - 1 = 2a \;\vee\; \exists b \;\; k+1 = 2b$
9. $\exists a \;\; k = 2a + 1 \vee \exists b \;\; k = 2b - 1$
10. In both cases k is odd

138

Indirect Proof Example

PROVE: The square of an even number is even.

1. Suppose k^2 is not even.
2. So k^2 is odd.
3. $\exists n \;\; k^2 = 2n + 1$
4. $\exists n \;\; k^2 - 1 = 2n$
5. $\exists n \;\; (k - 1)(k + 1) = 2n$
6. $2 \mid (k - 1)(k + 1)$
7. $2 \mid (k - 1) \;\vee\; 2 \mid (k + 1)$ since 2 is prime
8. $\exists a \;\; k - 1 = 2a \;\vee\; \exists b \;\; k+1 = 2b$
9. $\exists a \;\; k = 2a + 1 \vee \exists b \;\; k = 2b - 1$
10. In both cases k is odd
11. So k is not even

139

Rational Numbers
an Easier Characterization

Recall the set of rational numbers **Q** = the set of numbers with decimal expansion which is periodic past some point (I.e. repeatinginginginginging…)

Easier characterization

Q = { p/q | p,q are integers with $q \neq 0$ }

Prove that the sum of any irrational number with a rational number is irrational:

140