Problem 1. 50 points

Here are a couple of useful websites:

Use this one to check your hand calculation of the multiplicative modular inverse: e^{-1}: Link here.

Use this on to perform modular exponentiation. We are dealing with big numbers even for these toy examples and a regular calculator may give the wrong answer. Link here.

(a) Given the public key $e = 13, n = 77$ encrypt the message "HACKED" one letter at a time using ASCII to represent each letter. (Capitalization matters in ASCII)

(b) Decrypt the cyphertext you created in part (a) using the private key: $e^{-1} = 37$.

(c) Given primes p = 11 and q = 7, and $e = 13$ run through the RSA algorithm showing the encryption and decryption of the message "ACE" one letter at a time. Show the setup, encryption and decryption steps.

Solution

(a)

- ASCII representation of "HACKED" is 72 65 67 75 69 68.
- Formula for generating the cyphertext is $C = M^e \pmod{77}$
- $51 = 72^{13} \mod 77$
- $65 = 65^{13} \mod 77$
- $67 = 67^{13} \mod 77$
- $47 = 75^{13} \mod 77$
- $27 = 69^{13} \mod 77$
- $19 = 68^{13} \mod 77$
- The cyphertext is 51 65 67 47 27 19

(b)

- The cyphertext is 51 65 67 47 27 19.
- Formula for generating the decrypted message is $M = C^{e^{-1}} \pmod{77}$
- $72 = 51^{37} \mod 77$

- $65 = 65^{37} \mod 77$
- $67 = 67^{37} \mod 77$
- $75 = 47^{37} \mod 77$
- $69 = 27^{37} \mod 77$
- $68 = 19^{37} \mod 77$
- The message is 72 65 67 75 69 68 = "HACKED"

(c)

Bob sets up RSA:

- $n = p \cdot q = 11 \cdot 7 = 77$
- $\Phi(n) = \Phi(p)\Phi(q) = (p-1)(q-1) = 60)$
- Calculate e^{-1} using the extended Euclidean algorithm.
  $p_0 = 0, p_1 = 1, p_n = p_{n-2} - p_{n-1}q_{i-2} (\mathbf{mod}\ \Phi(n))$

  Each row in the following table is $n, t = q \cdot s + r, p_n$

n	t	q_n	s	r	p_n
0	60	13	4	8	**0**
1	13	8	1	5	**1**
2	8	5	1	3	-4
3	5	3	1	2	5
4	3	2	1	1	-9
5	2	1	2	0	14
6					-23

  $-23 \equiv 37 (\mathbf{mod}\ 60)$ since $-23 \mod 60 = 37 \mod 60$, or $60 - 23 = 37$.
  $e^{-1} = 37$.

- Bob makes e and n public.

,

Alice encrypts the message "ACE" and sends it to Bob:

- ACE in ASCII is 65 67 69
- $M^e (\mathbf{mod}\ n) \equiv C$
- $65^{13} (\mathbf{mod}\ 77) \equiv 65$
- $67^{13} (\mathbf{mod}\ 77) \equiv 67$

- $69^{13} (\textbf{mod } 77) \equiv 27$
- Alice sends Bob 65 67 27

Bob decrypts the cyphertext he received from Alice:

- $C^{e^{-1}} (\textbf{mod } n) \equiv M$
- $65^{37} (\textbf{mod } 77) \equiv 65$
- $67^{37} (\textbf{mod } 77) \equiv 67$
- $27^{37} (\textbf{mod } 77) \equiv 69$
- 65 67 69 in ASCII is "A" "C" "E".

Problem 2. 50 points

Prove using mathematical induction the following claims:

(a) Let P(n) be the property "n¢ can be obtained using 2¢ and 5¢ coins". Use *weak mathematical induction* to prove that P(n) is true for all integers $n \geq 4$.

(a)

Claim: $\forall n \in \mathbb{Z}^+ \wedge n \geq 4, \exists s, t \in \mathbb{Z}^+ \ni n = 2s + 5t$. (This statement is equivalent to P(n))

Proof. by induction on n.

The idea here is to show that whenever we have a combination of 2 and 5 cent coins that equal k cents we can always replace some of the existing coins with 5 or 2 cents coins in such a way that we get one more cent.

Base case: $n = 4$.

$4 = 2 \cdot 2 + 0 \cdot 5$. (Choose s to be 2)

QED for the base case.

Inductive step: $\exists s, t \in \mathbb{Z}^+ \ni k = 2s + 5t \implies \exists p, q \in \mathbb{Z}^+ \ni k + 1 = 2p + 5q$

There are three cases: k is odd or k is even; if k is even s is even otherwise t is even.

Case: k is odd:

$\text{odd}(k) \implies \text{odd}(t)$ (Since only an odd times an odd is odd)

Replacing one 5 with three 2s, i.e. increasing s by three (s+3= p) and decreasing t (t-1=q) by one results in $k + 1 = 2p + 5q$.

$\therefore \exists p, q \in \mathbb{N} \ni 2p + 5q = k + 1$

QED for the odd case

Case: k is even:

$\text{even}(s) \implies \text{even}(s) \vee \text{even}(t)$. (Since an even times an even or an odd times an even is even)

if s even, and not zero, then make: $p = s - 2$ and $q = t + 1$.

(i.e. replace two 2¢ coins with one 5¢ coin)

otherwise t is even and not zero so make: $p = s + 3$ and $q = t - 1$.

(i.e. replace one 5¢ coin with three 2¢ coins)

$\therefore \exists p, q \in \mathbb{N} \ni 2p + 5q = k + 1$

QED for the cases where k is even

□

(b) Use *weak mathematical induction* to prove that $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

Proof. by induction on n.

Base case: n = 0

$0 = \frac{0(0+1)}{2}$

QED for the base case

Inductive step:

$1+2+3+\ldots+k = \frac{k(k+1)}{2}$

$\implies 1+2+3+\ldots+k+(k+1) = \frac{(k+1)((k+1)+1)}{2}$

Proof

$$1+2+3+\ldots+k = \frac{k(k+1)}{2} \qquad \text{(Inductive Hypothesis)}$$

$$\therefore 1+2+3+\ldots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) \qquad \text{(Substitution)}$$

$$= \frac{k(k+1)+2(k+1)}{2} \qquad \text{(Addition of fractions)}$$

$$= \frac{k^2+k+2k+2)}{2} \qquad \text{(Multiplication)}$$

$$= \frac{k^2+3k+2)}{2} \qquad \text{(Addition)}$$

$$= \frac{(k+1)(k+2))}{2} \qquad \text{(Factoring)}$$

$$= \frac{(k+1)((k+1)+1))}{2} \qquad \text{(Addition)}$$

QED

$\square$

(c) Use *weak mathematical induction* to prove that $\forall n \geq 1, 3 \mid 2^{2n} - 1$.

Proof. (by induction on n).

Base case: n = 1

$3 \mid 2^{2(1)} - 1 \implies 3 \mid 4 - 1 = 3.$ (Definition of divides)

QED for the base case

Inductive step:

$3 \mid 2^{2k} - 1 \implies 3 \mid 2^{2(k+1)} - 1$

Proof

$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1$ (Rules of exponents)

$3 \mid 2^{2k} - 1$ (Inductive Hypothesis)

$3 \mid 2^{2k} - 1 \implies \exists m \in \mathbb{N} \ni 2^{2k} - 1 = 3m$ (Definition of divisibility)

$\therefore 2^2 \cdot 2^{2k} - 1 = 4 \cdot 3m$ (Substitution)

$3 \mid 4 \cdot 3m$ (Since 3 is a factor)

$\therefore 3 \mid 2^2 \cdot 2^{2k} - 1$ (Substitution)

$\therefore 3 \mid 2^{2(k+1)} - 1$ (Rules of exponents)

QED

□

(d) Use *strong mathematical induction* to prove that any integer greater than 1 is divisible by a prime number.

Proof. (by strong induction on n).

Base case: n = 2
$2 \mid 2 \wedge 2 \in$ Primes
QED for the base case
Inductive step:
$\forall m \in \mathbb{Z}, m < k, \exists p \in \text{Primes} \ni p \mid m \implies \exists p \in \text{Primes} \ni p \mid k$ (Strong Induction)
Proof
There are two cases. Either k is prime or k is composite.
k is prime:
$k|k \wedge k \in$ Primes
QED for k prime
k is composite:
$\exists S \subset \mathbb{N} \ni k = S_0 \cdot S_{|S|-1} \wedge S_0 \ldots S_{|S|-1} < k$ (Definition of composite)
$\forall s \in S \ni \exists p \in \text{Primes} \ni p|s.$ (Strong Inductive Hypothesis)
(If p is a factor of one of k's factors it is a factor of k)
$p \mid S_0 \cdot S_{|S|-1} = k \implies p|k.$
QED for k composite

□

(e) Use *strong mathematical induction* to prove that $\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+, \exists q, r \in \mathbb{N} \ni n = d \cdot q + r \wedge 0 \leq r < d$. You will need to use the *Well-Ordering Principle* P. 620 of Rosen.

Solution

Proof. (By the well-ordering principle).

Let S be the set $\{s \in \mathbb{Z}^+ \mid s = n - d \cdot k, k \in \mathbb{Z}\}$
Lemma 1: $|S| > 0$
Proof that S is not empty:
Two cases: $n \geq 0$ and $n < 0$
$n \geq 0:$
$n - 0 \cdot d = n \wedge n \geq 0$ ()
$\therefore n - 0 \cdot d \in S$
QED for $n \geq 0$
$n < 0:$
$n - n \cdot d = n(1 - d) \wedge n \geq 0 \wedge 1 - d \geq 0$ (Since d is a positive integer by assumption)
$\therefore n - n \cdot d \in S$
QED for Lemma 1
$\therefore$ S has a least element (By the well-ordering principle and S not empty)
Let r be the least element in S
$\therefore \exists q \in \mathbb{Z} \ni n - d \cdot q = r$ (By definition of S)
$\therefore n - d \cdot q = r \implies n = d \cdot q + r$ (Algebra)
Lemma 2: $r < d$
Proof that $r < d$ by contradiction
Assume $r \geq d$ (Negation of the hypothesis)
$\therefore n - d(q+1) = n - d \cdot q - d = r - d \geq 0$ (Algebra)
$\therefore n - d(q+1) \in S \wedge n - d(q+1) < r$
$\therefore n - d(q+1)$ is in S and
is less than the smallest element in S
$\Rightarrow\Leftarrow$
QED for Lemma 2
$\therefore n = d \cdot q + r, 0 \leq r < d$

$\square$