

Problem 1: Compute 55^{55}

- (a) mod 7,
- (b) mod 11, and
- (c) mod 13.
- (d) State the Chinese Remainder Theorem and use it to compute $55^{55} \bmod 1001$.

Solution: (a) Since $55 \bmod 7 = 6 = -1$, we have $55^{55} \bmod 7 = (-1)^{55} \bmod 7 = -1 \bmod 7 = 6$.

(b) Since $55 \bmod 11 = 0$, we have $55^{55} \bmod 11 = 0$ as well.

(c) Since $55 \bmod 13 = 3$ and $3^3 \bmod 13 = 27 \bmod 13 = 1$, we have $55^{55} \bmod 13 = 3$.

(d) The Chinese Remainder Theorem says that if the positive integers m_1, m_2 and m_3 are pairwise relatively prime then for any triple (a_1, a_2, a_3) of integers there is a unique integer solution x in the interval $0 \leq x \leq m_1 m_2 m_3 - 1$ of the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3}. \end{aligned}$$

Here, we seek the solution $x = 55^{55} \bmod 1001$ of three congruences

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ x &\equiv 0 \pmod{11} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

and $7 \cdot 11 \cdot 13 = 1001$. We decouple the congruences by guessing $x = x_1 \cdot 11 \cdot 13 + x_2 \cdot 7 \cdot 13 + x_3 \cdot 7 \cdot 11$, so the x_i 's satisfy three separate congruences

$$\begin{aligned} 11 \cdot 13 \cdot x_1 &\equiv 3 \cdot x_1 \equiv 6 \pmod{7} \\ 7 \cdot 13 \cdot x_2 &\equiv 3 \cdot x_2 \equiv 0 \pmod{11} \\ 7 \cdot 11 \cdot x_3 &\equiv -1 \cdot x_3 \equiv 3 \pmod{13}. \end{aligned}$$

By inspection or by finding inverses and multiplying, we find $x_1 = 2$, $x_2 = 0$ and $x_3 = -3$ so $x = 2 \cdot 11 \cdot 13 - 3 \cdot 7 \cdot 11 \equiv 55 \bmod 1001$.

Problem 2: Consider the following pseudocode:

```

procedure  $G$ (natural number  $n$ )
   $A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ ,     $B := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 
  while( $n > 0$ )
  begin
    if( $n \bmod 2 \neq 0$ ) then  $B := A \cdot B$ 
     $A := A \cdot A$ 
     $n := \lfloor n/2 \rfloor$ 
  end
  return  $B_{12}$ 
end

```

- (a) State the definition of an algorithm. Is G an algorithm? Why or why not?
- (b) Evaluate $G(0)$, $G(1)$, $G(2)$ and $G(3)$.

- (c) What function of n does $G(n)$ return in general?
 (d) What is its worst-case complexity in terms of n in big- O notation?

Solution: (a) An algorithm is a finite set of precise instructions for performing a computation or solving a problem. In particular, an algorithm must *terminate*. Since n is halved at each iteration of the while loop, G must terminate. Since G is a finite set of precise instructions, G is an algorithm.

(b) $G(0) = 0$, $G(1) = 1$, $G(2) = 1$, $G(3) = 2$.

(c) $G(n)$ returns the n th Fibonacci number f_n .

(d) G requires at most $2 \log_2(n)$ 2×2 matrix multiplications and floors, so the worst-case complexity is $W(n) = O(\log n)$.

Problem 3: (a) Show by applying logical equivalences that $((p \vee q) \wedge (p \rightarrow r)) \rightarrow (q \vee r)$ is a tautology. State which logical equivalence is used at each step.

(b) Prove that for any sets A , B and C we always have $(A \cup B) \cap (\bar{A} \cup C) \subset B \cup C$.

Solution: (a) By definition of implication, the given proposition is equivalent to

$$\neg((p \vee q) \wedge (\neg p \vee r)) \vee (q \vee r).$$

By de Morgan, this is equivalent to

$$(\neg(p \vee q) \vee \neg(\neg p \vee r)) \vee (q \vee r)$$

or after cancelling double negatives,

$$((\neg p \wedge \neg q) \vee (p \wedge \neg r)) \vee (q \vee r)$$

Using associativity and commutativity gives

$$(\neg p \wedge \neg q) \vee q \vee (p \wedge \neg r) \vee r$$

and by the distributive law, this is

$$((\neg p \vee q) \wedge (\neg q \vee q)) \vee ((p \vee r) \wedge (\neg r \vee r)).$$

By excluded middle and domination, this reduces to $(\neg p \vee q) \vee (p \vee r)$ and by associativity, commutativity and domination this is T .

(b) Define propositional functions $p(x) = "x \in A"$, $q(x) = "x \in B"$, and $r(x) = "x \in C"$. Apply part (a) and quantify over x to obtain the result.

Problem 4: (a) Encrypt the message $M = 2$ in the RSA code with $p = 3$, $q = 11$ and $e = 7$.

(b) Decrypt the coded message $C = 10$ in the RSA code of (a).

Solution: (a) $C = M^e \bmod pq = 2^7 \bmod 33 = 128 \bmod 33 = 29$.

(b) First, an inverse of $e = 7 \bmod (p-1)(q-1) = 7 \bmod 20$ is $d = 3$ by inspection. Thus the decoded message is $M = C^d \bmod 33 = 10^3 \bmod 33 = 1000 \bmod 33 = 10$.

Problem 5: Define a sequence S_n by $S_0 = 0$, $S_1 = 2$ and $S_{n+1} = nS_n + S_{n-1}$ for $n \geq 1$.

(a) Compute S_4 .

(b) Prove by induction that $\gcd(S_{n+1}^2, S_n^2) = 4$ for $n \geq 0$.

Solution:

(a) $S_2 = 1 \cdot S_1 + S_0 = 2$, $S_3 = 2 \cdot S_2 + S_1 = 6$, $S_4 = 3 \cdot S_3 + S_2 = 20$.

(b) The Fundamental Theorem of Arithmetic immediately implies that $\gcd(a^2, b^2) = \gcd(a, b)^2$. Therefore it suffices to prove that $\gcd(S_{n+1}, S_n) = 2$.

Base: Clearly $\gcd(S_1, S_0) = \gcd(2, 0) = 2$.

Induction: Fix $n > 0$ and assume the induction hypothesis $\gcd(S_n, S_{n-1}) = 2$. Then $\gcd(S_{n+1}, S_n) = \gcd(nS_n + S_{n-1}, S_n) = \gcd(S_{n-1}, S_n) = \gcd(S_n, S_{n-1})$ since $\gcd(qb + r, b) = \gcd(b, sb + r)$ for any $s \geq 0$.