University Discrete Mathematics · Practice Worksheet · tutorinmontreal.ca

Modular Arithmetic and Cryptography

Name: _____ Date: _____

Concepts

- Congruences and Arithmetic Modulo n
- Modular Inverses and Linear Congruences
- Fermat's Little Theorem and Modular Exponentiation (theory)
- RSA Encryption and Decryption

Congruences and Arithmetic Modulo n

1. Recall that for an integer $n \geq 2$, $a \equiv b \pmod{n}$ means $n \mid (a - b)$, and $a \bmod n$ is the remainder r with $0 \leq r < n$ and $a \equiv r \pmod{n}$.

a) Decide whether $83 \equiv -7 \pmod{15}$.

b) Decide whether $214 \equiv 4 \pmod{12}$.

c) Compute $(-45) \bmod 8$.

d) List every integer x with $-20 \leq x \leq 20$ and $x \equiv 3 \pmod{7}$.

2. Without a calculator and without multiplying out, find:

a) the remainder when $47 \cdot 58 + 39^2$ is divided by 11;

b) $2^{50} \bmod 7$;

c) the last digit of 7^{83}.

Modular Inverses and Linear Congruences

3. Use the extended Euclidean algorithm to find an inverse of 11 modulo 26, that is, an integer s with $0 \le s < 26$ and $11s \equiv 1 \pmod{26}$. Check your answer.

4. Solve each congruence, giving every solution modulo the stated modulus, or show that there is none.

a) $7x \equiv 5 \pmod{18}$

b) $12x \equiv 20 \pmod{28}$

c) $10x \equiv 7 \pmod{25}$

Fermat's Little Theorem and Modular Exponentiation

5. Fermat's little theorem states: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

a) Compute $3^{45} \bmod 17$ by repeated squaring: write 45 in binary, tabulate $3^1, 3^2, 3^4, \ldots \bmod 17$, and multiply the powers you need.

b) Use Fermat's little theorem to compute $7^{2026} \bmod 13$.

RSA Encryption and Decryption

6. In RSA, one chooses distinct primes p and q, sets $n = pq$, chooses e with $\gcd(e, (p-1)(q-1)) = 1$, and lets d be the inverse of e modulo $(p-1)(q-1)$. The public key is (n, e), the private key is d. A message is an integer m with $0 \le m < n$; it is sent as $c = m^e \bmod n$ and recovered as $m = c^d \bmod n$.

Take $p = 5$ and $q = 11$.

a) Compute n and $(p-1)(q-1)$, and explain why $e = 5$ is not an allowed choice.

b) With $e = 3$, find the private key d.

c) Encrypt the message $m = 8$.

7. An RSA key has public part $(n, e) = (77, 7)$ and private key $d = 43$. (A message m with $0 \le m < n$ is sent as $c = m^e \bmod n$ and recovered as $m = c^d \bmod n$.) You receive $c = 37$. Decrypt it by repeated squaring, and check your answer by re-encrypting it.

Synthesis — drawing on several topics in this unit

8. Find every x with $0 \le x < 13$ such that $5x \equiv 3^{100} \pmod{13}$.