Preparing for Midterm 1

- These problems are taken from the lectures to help you prepare for our upcoming midterm exam. You can find solutions to all of these in the lecture sketches.
- Additional, more exam-like, practice problems are also posted to our course website.

a is invertible modulo n $\iff$ [ ]

Example 1. Determine $4^{-1} \pmod{13}$.

Example 2. Solve $4x \equiv 5 \pmod{13}$.

(Bézout's identity) Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

[ ]

The integers x, y can be found using the **extended Euclidean algorithm**.

In particular, if $\gcd(a, b) = 1$, then $a^{-1} \equiv$ [ ].

Example 3. Find $d = \gcd(17, 23)$ as well as integers r, s such that $d = 17r + 23s$.

Example 4. Determine $17^{-1} \pmod{23}$.

Example 5. Determine $16^{-1} \pmod{25}$.

Definition 6. **Euler's phi function** $\phi(n)$ counts [ ].

If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) =$ [ ].

Example 7. Compute $\phi(35)$.

Example 8. Compute $\phi(100)$.

Armin Straub
straub@southalabama.edu

Our ultimate goal is to secure messaging (at least) against:

- [ ]
- [ ]

Example 9. **(affine cipher)** A slight upgrade to the shift cipher, we encrypt each character as

$$E_{(a,b)}: \quad x \mapsto ax + b \pmod{26}.$$

How does the decryption work? How large is the key space?

Example 10. Encrypt $HOLIDAY$ using a Vigenere cipher with key BAD.

Example 11. In a few words, describe the following common kinds of attacks:

- ciphertext only attack
- known plaintext attack
- chosen plaintext attack
- chosen ciphertext attack

Example 12. Alice sends the ciphertext $BKNDKGBQ$ to Bob. Somehow, Eve has learned that Alice is using the Vigenere cipher and that the plaintext is $ALLCLEAR$. Next day, Alice sends the message $DNFFQGE$. Crack it and figure out the key that Alice used! (What kind of attack is this?)

Example 13. **(substitution cipher)** In a substitution cipher, the key k is some permutation of the letters $A, B, ..., Z$. For instance, $k = FRA....$ Then we encrypt $A \to F$, $B \to R$, $C \to A$ and so on. How large is the key space?

Example 14. It seems convenient to add the space as a 27th letter in the historic encryption schemes. Can you think of a reason against doing that?

Theorem 15. **(Fermat's little theorem)**

Theorem 16. **(Euler's theorem)**

Example 17. Compute $3^{1003} \pmod{101}$.

Example 18. What are the last two (decimal) digits of 3^{7082}?

Example 19. Compute $3^{25} \pmod{101}$.

Example 20. Compute $2^{20} \pmod{41}$.

Example 21. Express 25 in base 2.

Example 22. Express 49 in base 2.

Example 23. What is $(31)_8$ in decimal?

Example 24. What is ASCII?

Example 25. Compute: $1011 \oplus 1111$

A **one-time pad** works as follows:

Example 26. Using a one-time pad with key $k = 1100, 0011$, what is the message $m = 1010, 1010$ encrypted to?

If a one-time pad is used exactly once to encrypt a message, then perfect ______ is achieved.

Example 27. Alice made a mistake and encrypted the two plaintexts m_1, m_2 using the same key k. How can Eve exploit that?

Using the one-time pad presents several challenges, including:

- ______
- ______
- ______
- ______

Example 28. Explain why a ciphertext only attack on the one-time pad is entirely hopeless. What about the other attacks?

Yet, the one-time pad by itself provides little protection of ______.

Example 29. Alice sends an email to Bob using a one-time pad. Eve knows that and concludes that, per email standard, the plaintext must begin with `To: Bob`. Eve wants to tamper with the message and change it to `To: Boo`, for a light scare. Explain how Eve can do that!

Example 30. One thing that makes the one-time pad difficult to use is that the key needs to be the same length as the plaintext. What if we have a shorter key and just repeat it until it has the length we need? Why is that a terrible idea?

A **stream cipher** works as follows:

(linear congruential generator)

From the seed x_0, we produce the sequence $x_{n+1} =$ [ ].

Example 31. Generate values using the linear congruential generator $x_{n+1} = 5x_n + 3 \pmod{8}$, starting with the seed $x_0 = 6$. What is the period?

Example 32. Explain the idea behind using a **nonce** in a stream cipher.

Example 33. Let's use the PRG $x_{n+1} = 5x_n + 3 \pmod{8}$ as a stream cipher with the key $k = 4 = (100)_2$. The key is used as the seed x_0 and the keystream is $\mathrm{PRG}(k) = x_1 x_2 \ldots$ (where each x_i is 3 bits). Encrypt the message $m = (101\ 111\ 001)_2$.

Example 34. Eve intercepts the ciphertext $c = (111\ 111\ 111)_2$. It is known that a stream cipher with PRG $x_{n+1} = 5x_n + 3 \pmod{8}$ was used for encryption. Eve also knows that the plaintext begins with $m = (110\ 1\ldots)_2$. Help her crack the ciphertext!

(linear feedback shift register (LFSR)

From the seed $(x_1, x_2, \ldots, x_\ell)$, where each x_i is one bit, we produce the sequence

$$x_{n+\ell} \equiv \boxed{}.$$

Example 35. Which sequence is generated by the LFSR $x_{n+2} \equiv x_{n+1} + x_n \pmod{2}$, starting with the seed $(x_1, x_2) = (0, 1)$? What is the period?

Example 36. Which sequence is generated by the LFSR $x_{n+3} \equiv x_{n+1} + x_n \pmod{2}$, starting with the seed $(x_1, x_2, x_3) = (0, 0, 1)$? What is the period?

Example 37. The recurrence $x_{n+31} \equiv x_{n+28} + x_n \pmod{2}$, with a nonzero seed, generates a sequence that has period [ ].

Example 38. Eve intercepts the ciphertext $c = (1111\ 1011\ 0000)_2$ from Alice to Bob. She knows that the plaintext begins with $m = (1100\ 0\ldots)_2$. Eve thinks a stream cipher using a LFSR with $x_{n+3} \equiv x_{n+2} + x_n \pmod{2}$ was used. If that's the case, what is the plaintext?

Armin Straub
straub@southalabama.edu

A PRG is **predictable** if

Example 39. Let us consider a baby version of CSS. Our PRG uses the LFSR $x_{n+3} \equiv x_{n+1} + x_n \pmod{2}$ as well as the LFSR $x_{n+4} \equiv x_{n+2} + x_n \pmod{2}$. The output of the PRG is the output of these two LFSRs added with carry.

If we use $(0, 0, 1)$ as the seed for LFSR-1, and $(0, 1, 0, 1)$ for LFSR-2, what are the first 10 bits output by our PRG?

Example 40. In each case, determine if the stream could have been produced by the LFSR $x_{n+5} \equiv x_{n+2} + x_n \pmod{2}$. If yes, predict the next three terms.

(STREAM-1) $..., 1, 0, 0, 1, 1, 1, 1, 0, 1, ...$ (STREAM-2) $..., 1, 1, 0, 0, 0, 1, 1, 0, 1, ...$

Theorem 41. (Chinese Remainder Theorem)

Example 42. Solve $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Example 43. Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$

Example 44. Solve $x \equiv 4 \pmod{5}$, $x \equiv 10 \pmod{13}$.

Example 45. Let $p, q > 3$ be distinct primes.

(a) Show that $x^2 \equiv 9 \pmod{p}$ has exactly two solutions (i.e. ± 3).

(b) Show that $x^2 \equiv 9 \pmod{pq}$ has exactly four solutions (± 3 and two more solutions $\pm a$).

Example 46. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Example 47. Determine all solutions to $x^2 \equiv 4 \pmod{105}$.

Example 48. List all quadratic residues modulo 11.

Example 49. List all quadratic residues modulo 15. How many invertible quadratic residues are there? Explain!

Example 50. Let p, q, r be distinct odd primes.

- The number of invertible residues modulo n is ______.
- The number of invertible quadratic residues modulo p is ______.
- The number of invertible quadratic residues modulo pq is ______.

Armin Straub
straub@southalabama.edu

- The number of invertible quadratic residues modulo pqr is [ ].

(Blum-Blum-Shub PRG) Let $M = pq$ where p, q are large primes $\equiv 3 \pmod{4}$.
From the seed y_0,

Example 51. Generate random bits using the B-B-S PRG with $M = 77$ and seed 3.

Theorem 52. -1 is a quadratic residue modulo (an odd prime) $p \iff$ [ ].

Fermat primality test

Input:

Output:

Algorithm:

Example 53. If n is composite, then $a \pmod{n}$ is called a **Fermat liar** if [ ].

Example 54. A composite number n is an **absolute pseudoprime** if [ ].

Theorem 55. (prime number theorem) Up to x, there are roughly [ ] many primes.

Armin Straub
straub@southalabama.edu