1 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.
- I will also post additional practice problems before the end of the week.

a is invertible modulo n $\iff$ [ ]

Example 1. Solve $3x \equiv 2 \pmod 5$.

(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 2. Solve $16x \equiv 3 \pmod{25}$.

Example 3. Find the modular inverse of 17 modulo 23.

Example 4.

(a) Using the extended Euclidean algorithm, determine $46^{-1} \pmod{99}$.

(b) Solve $81x \equiv 4 \pmod{101}$.

Definition 5. 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 6. Compute $\phi(100)$.

Example 7. Evaluate $\phi(2016)$ and $\phi(10^n)$.

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

- [ ]

Armin Straub
straub@southalabama.edu

-

Example 8. Encrypt $HOLIDAY$ using a Vigenere cipher with key BAD.

Example 9. The message $QSYNGGI$ was encrypted by your friend Alice using a Vigenere cipher with the key USA. Decrypt it.

Example 10. What a terrible blunder... Explain what is wrong, and correct the mistake!

$$\text{(incorrect!)} \quad 10^9 \equiv 3^2 = 9 \equiv 2 \pmod 7$$

Theorem 11. (Fermat's little theorem)

Theorem 12. (Euler's theorem)

Example 13. Compute $3^{1003} \pmod{101}$.

Example 14. Compute $3^{25} \pmod{101}$.

Example 15. What are the last two (decimal) digits of 3^{7082}?

Example 16. Compute $2^{20} \pmod{41}$.

Example 17. Compute $99^{307} \pmod{84}$.

Example 18. (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 19. (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 20. 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?

Example 21. Express 25 in base 2.

Example 22. Express 49 in base 2.

Armin Straub
straub@southalabama.edu

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

Example 24. What is $(FACE)_{16}$ in decimal?

Example 25. In a few words, describe the following common kinds of attacks:

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

Example 26. Alice sends the ciphertext $B\,K\,N\,D\,K\,G\,B\,Q$ to Bob. Somehow, Eve has learned that Alice is using the Vigenere cipher and that the plaintext is $A\,L\,L\,C\,L\,E\,A\,R$. Next day, Alice sends the message $D\,N\,F\,F\,Q\,G\,E$. Crack it and figure out the key that Alice used! (What kind of attack is this?)

Example 27. What is ASCII?

Example 28. Compute: $1011 \oplus 1111$

Example 29. Why is $a \oplus b \oplus b = a$?

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

Example 30. Using a one-time pad, what is the message $m = 1010, 1010$, using the key $k = 1100, 0011$, encrypted to?

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

Example 31. 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:

- [ ]
- [ ]
- [ ]

Armin Straub
straub@southalabama.edu

-

Example 32. 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 33. 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 34. 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 35. 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 36. Observe that the sequence produced by the linear congruential generator $x_{n+1} = ax_n + b \pmod m$ must repeat, at the latest, after m terms. (Why?!)

One can give precise conditions on a, b, m to achieve a full period m. Namely, this happens if and only if $\gcd(b, m) = 1$ and $a - 1$ is divisible by all primes (as well as 4) dividing m.

(a) Generate values using a linear congruential generator $x_{n+1} = 2x_n + 1 \pmod{10}$, starting with the seed $x_0 = 5$. When do they repeat? Is that consistent with the mentioned condition?

(b) What are possible values for a so that the linear congruential generator $x_{n+1} = ax_n + 11 \pmod{100}$ has period 100?

(c) As mentioned above, glibc uses $a = 1103515245$, $b = 12345$, $m = 2^{31}$. After how many terms will the sequence start repeating?

Example 37. Explain the idea behind using a **nonce** in a stream cipher.

Example 38. 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 39. Similarly, let's use the PRG $x_{n+1} = 9x_n + 5 \pmod{64}$ as a stream cipher with the key $k = 4 = (100)_2$ and nonce $5 = (101)_2$. The key prefixed with the nonce is used as the seed x_0, so that the keystream is $\mathrm{PRG}(\mathrm{nonce}, k) = x_1 x_2 \ldots$ (each x_i is now 6 bits).

Example 40. 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 41. 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 42. 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 43. 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) $\ldots, 1, 0, 0, 1, 1, 1, 1, 0, 1, \ldots$ (STREAM-2) $\ldots, 1, 1, 0, 0, 0, 1, 1, 0, 1, \ldots$

Example 44. One can also consider nonlinear recurrences (it mitigates some issues). Use $x_{n+3} \equiv x_{n+2}x_n + x_{n+1} \pmod{2}$ to generate some numbers.

A PRG is **predictable** if

Example 45. 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 46. List all quadratic residues modulo 11.

Example 47. List all quadratic residues modulo 15. How many invertible quadratic residues are there? Explain!

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

Example 48. Generate random bits using the B-B-S PRG with $M = 77$ and seed 3.

Example 49. Generate random bits using the B-B-S PRG with $M = 209$ and seed 10. What is the period of the generated sequence? (Then repeat with seed 25.)

Example 50.

(a) List all invertible quadratic residues modulo 21. Then (as in B-B-S) compute the square of all these residues.

(b) Repeat the first part modulo 33 and modulo 35. When computing the squares of these, do you notice a difference modulo 35?

(c) How many invertible quadratic residues are there modulo 707?

Example 51.

(a) If $x \equiv 3 \pmod{10}$, what can we say about $x \pmod 5$?

(b) If $x \equiv 3 \pmod 7$, what can we say about $x \pmod 5$?

Theorem 52. (Chinese Remainder Theorem)

Example 53. Solve $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$.

Example 54. Solve $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

Example 55.

(a) Solve $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod{25}$.

(b) Solve $x \equiv -1 \pmod 4$, $x \equiv 2 \pmod 7$, $x \equiv 0 \pmod 9$.

Example 56.

(a) Let $p > 3$ be a prime. Show that $x^2 \equiv 9 \pmod p$ has exactly two solutions (i.e. ± 3).

(b) Let $p, q > 3$ be distinct primes. Show that $x^2 \equiv 9 \pmod{pq}$ alwas has exactly four solutions (± 3 and two more solutions $\pm a$).

Example 57. Let m, n be coprime. Show that a is a quadratic residue modulo mn if and only if a is a quadratic residue modulo both m and n.

Example 58. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Example 59. Determine the modular inverse of $17 \pmod{42}$ in the following three ways:

(a) Directly, using the Euclidean algorithm.

(b) Using Euler's theorem and binary exponentiation.

(c) With the help of the Chinese remainder theorem.

Example 60. Compute $7^{111} \pmod{90}$ in the following three different ways:

(a) Directly, using binary exponentiation.

(b) With the help of Euler's theorem.

(c) With the help of the Chinese remainder theorem (as well as Euler's theorem).

Definition 61. The **multiplicative order** of an invertible residue a modulo n is

.

Lemma 62. If $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$, then .

Corollary 63. The multiplicative order of a modulo n divides .

Definition 64. a is said to be **primitive root** modulo n if .

Example 65. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Example 66. Determine the orders of each (invertible) residue modulo 7. In particular, determine all primitive roots modulo 7.

Lemma 67. If $x \pmod{n}$ has (multiplicative) order k, then x^a has order .