Lecture 32

Instructor's Comments: This is a make up lecture. You can choose to cover many extra problems if you wish or head towards cryptography. I will probably include the square and multiply algorithm at some point as an extra topic.

Handout or Document Camera or Class Exercise

Which of the following is equal to $[53]^{242} + [5]^{-1}$ in $\mathbb{Z}_7$?

(Do not use a calculator.)

A) [5]

B) [4]

C) [3]

D) [2]

E) [1]

Solution: Note that

$$\begin{aligned} 53^{242} + 5^{-1} &\equiv 4^{242} + 3 \pmod 7 \\ &\equiv 4^2 \cdot 4^{240} + 3 \pmod 7 \\ &\equiv 2 \cdot (4^6)^{40} + 3 \pmod 7 \\ &\equiv 2 \cdot 1^{40} + 3 \pmod 7 \\ &\equiv 5 \end{aligned}$$

Instructor's Comments: This is the 5-7 minute mark.

Theorem: Splitting the Modulus (SM) Let m and n be coprime positive integers. Then, for any integers x and a, we have

$$x \equiv a \pmod{m}$$
$$x \equiv a \pmod{n}$$

simultaneously if and only if $x \equiv a \pmod{mn}$.

Proof: ($\Leftarrow$) Assume that $x \equiv a \pmod{mn}$. Then $mn \mid (x - a)$. Since $m \mid mn$, by transitivity, we have that $m \mid (x-a)$ and hence $x \equiv a \pmod{m}$. Similarly, $x \equiv a \pmod{n}$.

($\Rightarrow$) Assume that $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$. Note that $x = a$ is a solution. Since $\gcd(m, n) = 1$, by the Chinese Remainder Theorem, $x \equiv a \pmod{mn}$ gives all solutions.

Instructor's Comments: This is the 15 minute mark.

Handout or Document Camera or Class Exercise

For what integers is $x^5 + x^3 + 2x^2 + 1$ divisible by 6?

Solution: We want to solve $x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 6$. By Splitting the Modulus, we see that

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 2$$
$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 3$$

Using equation 1 and plugging in $x \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 2$ gives in both cases that

$$x^5 + x^3 + 2x^2 + 1 \equiv 1 \pmod 2$$

Therefore, $x^5 + x^3 + 2x^2 + 1$ is never divisible by 6. ■

Instructor's Comments: This is the 25 minute mark. From here you can choose to do more practice and have a full lecture on Cryptography or just do a half lecture on cryptography.

Cryptography

Note: The practice/study of secure communication.

Alice wants to communicate with Bob and receive messages from Bob but Eve is listening to all the messages they send to each other.

Instructor's Comments: Include a picture

Alice needs to encrypt messages to Bob so that even if Eve can see them, she cannot read them. However Bob needs to be able to read them and so needs a way to decrypt them.

Note: A cryptosystem should not depend on the secrecy of the methods of encryption and decryption used (except for possibly secret keys). The method must be assumed to be known by all.

Private Key Cryptography

Agree before hand on a secret encryption and decryption key.

Instructor's Comments: Mention ASCII encryption. Break up messages into many chunks and send those chunks.

Example: Caesar Cipher. Map a plain text message M to a ciphertext (encrypted message) given by

$$C \equiv M + 3 \pmod{26}$$

where $0 \le C \le 26$. In this way, one can encrypt letters to new letters. This worked well for Caesar mainly because most soldiers could not read (so even an unencrypted message might not have been understood).

Example: $APPLE$ gets translated as a sequence of numbers $0, 15, 15, 11, 4$ then encrypted by adding 3 to get $3, 18, 18, 14, 7$ and then converted back to letters $DSSOH$.

Cons of Private Key Cryptography

(i) Tough to share private key before hand.

(ii) Too many private keys to store.

(iii) Difficult to communicate with strangers.

Public Key Cryptography

Analogy: Pad lock. A pad lock is easy to lock but difficult to unlock without the key. The main paradigm here is as follows:

(i) Alice produces a private key d and a public key e.

(ii) Bob uses the public key e to take a message M and encrypt it to some ciphertext C

(iii) Bob then sends C over an insecure channel to Alice.

(iv) Alice decrypts C to M using d.

Note:

(i) Encryption and decryption are inverses to each other.

(ii) d and e are different,

(iii) Only d is secret.

Instructor's Comments: This is the 40 minute mark - maybe the 50 minute mark

Question: What makes a problem hard?

Instructor's Comments: Something along the lines of the first thing you try doesn't work, a problem that has resisted proof for many years etc.

Example: Given the number 1271, find it's prime factorization.

Instructor's Comments: The answer is 31 times 41. The point here is that even for small numbers humans struggle with this. For not-very-large numbers, even computers struggle.

Factoring a number is a difficult problem and helps form the basis for RSA. If we could factor numbers easily, the RSA encryption we will talk about in the next lecture would be hard.

Instructor's Comments: This next question is completely optional as well. It doesn't add much to RSA. Question: Given $2^n \equiv 9 \pmod{11}$, find n.

Solution: The answer is $n = 6$. However this isn't the real point of this question. The point is that to find 6, you likely tried all the possibilities from

1 to 6 reducing reach time. This problem in general, that is, given a, b and $a^n \in \mathbb{N}$ for some $n \in \mathbb{N}$ to determine n is called the Discrete Logarithm Problem. There is currently no known efficient algorithm to solve it. Solving this would also help break the RSA encryption scheme.

Instructor's Comments: This is probably the 50 minute mark but if not, have fun with the square and multiply algorithm below. This topic is completely optional (as of W2016)

Square and Multiply Algorithm

The idea of this algorithm is to enable computers to compute large powers of integers modulo a natural number n quickly.

Example: Compute $5^{99} \pmod{101}$

Solution: First, we compute successive square powers of 5:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{101}\\
5^2 &\equiv 25 \pmod{101}\\
5^4 &\equiv (25)^2 \equiv 625 \equiv 19 \pmod{101}\\
5^8 &\equiv (19)^2 \equiv 361 \equiv 58 \pmod{101}\\
5^{16} &\equiv (58)^2 \equiv 31 \pmod{101}\\
5^{32} &\equiv (31)^2 \equiv 52 \pmod{101}\\
5^{64} &\equiv (52)^2 \equiv 78 \pmod{101}
\end{aligned}$$

Now, write 99 in binary, that is, as a simple sum of powers of 2 with no power of 2 repeated.

$$\begin{array}{ll}
64 \le 99 < 128 & \text{Replace } 99 \text{ with } 99 - 64 = 35\\
32 \le 35 < 64 & \text{Replace } 35 \text{ with } 35 - 32 = 3\\
2 \le 3 < 4 & \text{Replace } 3 \text{ with } 3 - 2 = 1\\
1 \le 1 < 2 & \text{Replace } 1 \text{ with } 1 - 1 = 0
\end{array}$$

Thus, $99 = 64 + 32 + 2 + 1 = 2^6 + 2^5 + 2^1 + 2^0$. Hence,

$$\begin{aligned}
5^{99} &\equiv 5^{64} \cdot 5^{32} \cdot 5^2 \cdot 5^1 \pmod{11}\\
&\equiv 78 \cdot 52 \cdot 25 \cdot 5 \pmod{11}\\
&\equiv 81 \pmod{11}
\end{aligned}$$

Instructor's Comments: Note the minimal number of computations needed. In general, it would be 98 computations. Here it's 6 + 3 =9 computations. A huge savings.

Handout or Document Camera or Class Exercise

(i) Show that $x = 2^{129}$ solves $2x \equiv 1 \pmod{131}$.

(ii) Use the square and multiply algorithm to find the remainder when 2^{129} is divided by 131.

(iii) Solve $2x \equiv 3 \pmod{131}$ for $0 \leq x \leq 130$.

Solution:

(i) By Fermat's Little Theorem (valid since $\gcd(2, 131) = 1$,

$$2(2^{129}) \equiv 2^{130} \equiv 1 \pmod{131}$$

(ii) First, we create a chart of the powers of 2:

$$\begin{aligned}
2^1 &\equiv 2 \pmod{131} \\
2^2 &\equiv 4 \pmod{131} \\
2^4 &\equiv 16 \pmod{131} \\
2^8 &\equiv 256 \equiv -6 \pmod{131} \\
2^{16} &\equiv (-6)^2 \equiv 36 \pmod{131} \\
2^{32} &\equiv (36)^2 \equiv 1296 \equiv -14 \pmod{131} \\
2^{64} &\equiv (-14)^2 \equiv 196 \equiv 65 \pmod{131} \\
2^{128} &\equiv (65)^2 \equiv 5^2 \cdot 13^2 \equiv 25 \cdot 169 \equiv 25 \cdot 38 \\
&\equiv 5 \cdot 190 \equiv 5 \cdot 59 \equiv 295 \equiv 33 \pmod{131}
\end{aligned}$$

Hence, $2^{129} \equiv 2^{128} \cdot 2^1 \equiv 33 \cdot 2 \equiv 66 \pmod{131}$.

(iii) Since $2 \cdot 66 \equiv 132 \equiv 1 \pmod{131}$, we see that $2 \cdot (66 \cdot 3) \equiv 3 \pmod{131}$ and since $66 \cdot 3 \equiv 198 \equiv 67 \pmod{131}$, we have completed the question. ■