Exercise Worksheet 3

November 21, 2022

1 Exercise 1

Use an efficient method to find an integer x that satisfies all of the following congruences simultaneously:

$$\begin{aligned} x &\equiv 1903 \pmod{51893} \\ x &\equiv 50491 \pmod{88411} \\ x &\equiv 48327 \pmod{96221} \end{aligned}$$

2 Exercise 2

Use Fermat's little theorem to demonstrate that

$$n = 393886917492300727037507589786141066780609032330563241735955813297922747315 63$$

is not prime.

3 Exercise 3

Use the Davis–Putnam procedure on the following clauses (represented by sets of literals) and determine if they are satisfiable or not:

$$\{\neg a, b, c\}, \{a, \neg b, d\}, \{\neg a, e\}, \{\neg d, \neg e\}, \{a, b, \neg c\}, \{c, \neg e\}$$

Choose variables in alphabetical order $a, b, c, \ldots$ when you have a choice of variable. Write down the new set of clauses every time the set changes.

4 Exercise 4

Suppose $p = 8796093022237$ and 10 people were given the following (α_i, β_i) pairs from the secret sharing scheme discussed in lecture:

$$(7254903237010, 3093846237950)$$
$$(4048558931707, 5993666701411)$$
$$(5246488265733, 5708406725900)$$
$$(4629861869950, 641074604855)$$
$$(5892756556784, 6983307202977)$$
$$(7655782796374, 1381308378374)$$
$$(3751466424183, 8337044522816)$$
$$(3555354811972, 3049046691536)$$
$$(1824417652410, 8663121656745)$$
$$(49537969121, 2439287167386)$$

Find the secret number using the secret recovery process. Interpret the secret as a base 27 number with `A` $= 1$, `B` $= 2$, etc. What is the secret passphrase?

Hint: Once you find the secret $s \in \mathbb{F}_p$ you can convert it to an base-27 integer using `Integer(s).digits(base=27)`.

[1]:
```
n = 10
p = 8796093022237

alpha = [7254903237010,
 4048558931707,
 5246488265733,
 4629861869950,
 5892756556784,
 7655782796374,
 3751466424183,
 3555354811972,
 1824417652410,
 49537969121]

beta = [3093846237950,
 5993666701411,
 5708406725900,
 641074604855,
 6983307202977,
 1381308378374,
 8337044522816,
 3049046691536,
 8663121656745,
 2439287167386]
```