CS 4823: Homework #4

Due on February 16, 2018

Christopher Tse

Problem 1

Compute the subgroup generated by $2 + 17\mathbb{Z}$ in $(\mathbb{Z}/17\mathbb{Z})^*$.

Solution

$2^0 \ mod\ 17 = 1$
$2^1 \ mod\ 17 = 2$
$2^2 \ mod\ 17 = 4$
$2^3 \ mod\ 17 = 8$
$2^4 \ mod\ 17 = 16$
$2^5 \ mod\ 17 = 15$
$2^6 \ mod\ 17 = 13$
$2^7 \ mod\ 17 = 9$
$2^8 \ mod\ 17 = 1$

Therefore, the subgroup is $1 \to 2 \to 4 \to 8 \to 16 \to 15 \to 13 \to 9 \to 1$

Problem 2

Determine the order of all the elements in $(\mathbb{Z}/15\mathbb{Z})^*$.

Solution

Unit group of $(\mathbb{Z}/15\mathbb{Z})^*$ is $\{1, 2, 4, 7, 8, 11, 13, 14\}$

$1^1 = 1 \ mod\ 15 = 1 \Rightarrow$ order 1
$2^4 = 16 \ mod\ 15 = 1 \Rightarrow$ order 4
$4^2 = 16 \ mod\ 15 = 1 \Rightarrow$ order 2
$7^4 = 2401 \ mod\ 15 = 1 \Rightarrow$ order 4
$8^4 = 4096 \ mod\ 15 = 1 \Rightarrow$ order 4
$11^2 = 121 \ mod\ 15 = 1 \Rightarrow$ order 2
$13^4 = 28561 \ mod\ 15 = 1 \Rightarrow$ order 4
$14^2 = 196 \ mod\ 15 = 1 \Rightarrow$ order 2

Problem 3

In Sage, after initiation:

```
sage: R = Integers(238759164598236456438265456485648 7)
sage: a = 2097348274652489745829645 84
sage: b = 8345748957482365826487524754 85
```

If we run `sage: R(a)^b` we get the answer 23416702453836441953378308613 52166. However, if we run `sage: R(a^b)` we get "RuntimeError". Explain why by estimating how much disk space (in GBytes) is needed to store the result of a^b in binary.

Solution

The number of bits required to store a^b in binary is $\log_2(a^b)$. While normally this logarithm is too large to compute, we can use the logarithm exponent rule.

$$\begin{aligned}\log_2(a^b) &= b\log_2(a)\\ &= 834574895748236582648752475485\log_2(2097348274652489745829645 84)\\ &= 7.297\times 10^{31}\end{aligned}$$

The number of bits required to store a^b is approximately 7.297×10^{31} bits, or approximately 9.122×10^{21} gigabytes.

Problem 4

Prove that RSA-1024 is a composite number using the Fermat Little Theorem with $a =$ your id number.

Solution: Proof by contradiction

Assume $p =$ RSA-1024 = 135066410865995223349603216278805969938881475
605667027524485143851526510604859533833940287150571909441798207282 16
447155137368041970396419174304649658927425623934102086438320211037 29
587257623585096431105640735015081875106765946292055636855294752135 00
852879416377328533906109750544334999811150056977236890927563

According to Fermat's Little Theorem, if p is prime and $a \nmid p$, then $a^{p-1} \equiv 1(mod\ p)$, or $a^p \equiv a(mod\ p)$.

Since $a^p\ mod\ p$ is too large to compute, we can first take $a\ mod\ p$ then raise it to the p-th power. In this case, $a\ mod\ p = a$. According to Fermat's Little Theorem then,

$$\begin{aligned}(a\ mod\ p)^p &= a\\ a^p &\neq a\end{aligned}$$

Since $a^p \neq a$, Fermat's Little Theorem does not hold true for p, therefore p is not a prime and is composite.