CS 8803 GA 09/11/2017

Problem Set 2

Instructor: Prof. Eric Vigoda *Tiancheng Gong*

Problem 1 DPV 1.12

Answer:

Since 3 is prime, by Fermat's Little Theorem (or by observation) we know that $2^2 \equiv 1 \mod 3$. We'll use this fact in the following manner:
Answer:

$$2^{2^{2006}} \equiv 2^{2\times 2^{2005}} \equiv \left(2^2\right)^{2^{2005}} \equiv (1)^{2^{2005}} \equiv 1 \mod 3$$

Problem 2 DPV 1.25

By Fermat's Little Theorem, since 127 is prime we know that $2^{126} \equiv 1 \mod 127$. To use this fact we need to find the inverse of $2 \mod 127$. Since $gcd(2, 127) = 1$ hence $2^{-1} \mod 127$ exists, and observe that $2^{-1} \equiv 64 \mod 127$. Using these facts we have:
Answer:

$$2^{125} \equiv 2^{126} \times 2^{-1} \equiv 1 \times 64 \equiv 64 \mod 127$$

Problem 3 DPV 1.20

Answer:

1. $4 \times 20 - 1 \times 79 = 1 \quad \Rightarrow \quad 20^{-1} \equiv 4 \mod 79$
2. $21 \times 3 - 1 \times 62 = 1 \quad \Rightarrow \quad 3^{-1} \equiv 21 \mod 62$
3. The inverse doesn't exist since $\gcd(21, 91) = 7 \neq 1$.
4. $5 \times 14 - 3 \times 23 = 1 \quad \Rightarrow \quad 5^{-1} \equiv 14 \mod 23$

Problem 4 DPV 1.22

Claim: If a has an inverse modulo b, then b has an inverse modulo a.

Proof:

If a has an inverse modulo b, then $\gcd(a, b) = 1$, which indicates b has an inverse modulo a as well.
Alternative proof:
Let $c \in \mathbb{Z}$ such that $c \equiv a^{-1} \mod b$, then there exists $d \in \mathbb{Z}$ such that $ca + db = 1$.
Mod both sides with a and we get $ca + db \equiv db \equiv 1 \mod a$, which implies d is an inverse of b modulo a. The claim is proved.

Problem 5 DPV 1.28

Answer:

Given $p = 7$ and $q = 11$, we have $(p-1)(q-1) = 60$.
We try $e = 2, 3, 5, 7, \ldots$, and $e = 7$ is the first one that has an inverse module 60 since $\gcd(7, 60) = 1$.
And using the Extended-Euclid Algorithm covered in the lecture, we can find $d \in \mathbb{Z}$ such that $d \equiv e^{-1} \mod 60$. The answer is $d = 43 \equiv 7^{-1} \mod 60$, which can be verified by $43 \times 7 - 5 \times 60 = 1$.

Problem 6 DPV 1.42

Claim: The new cryptosystem using only p is not secure.

Proof:

Let p be an n-bit number.

Given p, e and $m^e \mod p$, we can first compute the inverse of e modulo $p-1$ using the Extended-Euclid Algorithm in $O(n^3)$ time. Let the inverse be a, and we have $ae + b(p-1) = 1$.

According to the Fermat's Little Theorem, we have $m^{p-1} \equiv 1 \mod p$ since p is a prime.

Thus we can decrypt the message by $(m^e)^a \equiv m^{ae} \equiv m \cdot m^{-b(p-1)} \equiv m \mod p$. Since we are given $m^e \mod p$, which is at most $\log(p)$ bits and $a \leq p-1$ (otherwise we can subtract $p-1$ from a to get a smaller inverse), the computation time for this step is $O(n^3)$.

The total running time for this algorithm is $O(n^3) + O(n^3) = O(n^3)$, which is a polynomial time for the input space ($\log p = n$).