Math 480 (Spring 2007): Practice Midterm

Friday, April 20, 2007

There are 5 problems. Each problem is worth 6 points and parts of multipart problems are worth equal amounts. You must do all problems entirely by hand by the end of class without using notes, a calculator, or anything else except a pencil or pen. Every problem has a *specific numerical answer* – i.e., there are no abstract proof questions, though the theory you learned in the class will definitely help you to solve the problems. Some potentially useful calculations are listed at the bottom of the page. *Answers are on the back – do not look until you've done all problems. Do this practice exam under timed exam-like conditions!*

1. Find a positive integer x such that
$$\begin{aligned} x &\equiv 9 \pmod{19}, \text{ and} \\ x &\equiv 26 \pmod{97}. \end{aligned}$$

2. (a) Is the number 667 prime? Explain why or why not? (You may use, without proof, that $2^{666} \equiv 179 \pmod{667}$.)
   (b) Is the number 10967 prime? Explain why or why not?

3. (a) Nikita's RSA public key is $(n, e) = (55, 3)$. Encrypt the number 7 to her.
   (b) For the above public key, figure out what Nikita's RSA private key must be.
   (c) Nikita receives the encrypted message 3 (mod 55). Decrypt it using the private key from part (b).

4. (a) Compute $\gcd(91, 112)$ using any algorithm at all (even being "psychic", i.e., no proof required – just get the right answer).
   (b) Illustrate how to use the extended Euclidean algorithm to find integers x and y such that $112x - 91y = 14$.

5. You and Michael decide to agree on a secret number using the Diffie-Hellman key exchange. You together agree on the prime number $p = 23$ and primitive root $g = 5$. You choose the number $n = 5$ and Michael chooses a random number m and announces that $g^m \equiv 2 \pmod{23}$. What is the secret key that you agree on?

Some potentially useful calculations, which you may assume above:

```
sage: print prime_range(100)  # table of primes up to 100.
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
 67, 71, 73, 79, 83, 89, 97]
sage: Mod(9,19)^(-1)
17
sage: Mod(26,97)^(-1)
56
sage: Mod(2, 667)^666
179
sage: Mod(2, 667)^667
358
sage: Mod(3,55)^27
42
```

Numerical Answers

```
Problem 1:
sage: x = crt(9,26,19,97) % (19*97); x
123
sage: x%19
9
sage: x%97
26

Problem 2:
sage: is_prime(667)
False
sage: factor(667)
23 * 29

sage: # Note that you could use the divisibility by 11 test from the homework.
sage: is_prime(10967)
False
sage: factor(10967)
11 * 997

Problem 3:
sage: Mod(7,55)^3
13
sage: d = Mod(3,euler_phi(55))^(-1); d
27
sage: Mod(3,55)^d
42

Problem 4:
sage: gcd(91,112)
7
sage: g,x,y=xgcd(112,-91)
sage: 112*x -91*y
7
sage: (2*x,2*y)
(-8, -10)

Problem 5:
sage: Mod(2,23)^5
9
```