Math 480 (Spring 2007): In-Class Midterm

Wednesday, April 25, 2007

There are five problems. Each problem is worth 6 points and parts of multipart problems are worth equal amounts. You must do all problems *entirely by hand without using notes, a calculator, or anything else except a pencil or pen.*

Many useful calculations are **listed on the last page**. Be sure to quickly skim through the whole exam before starting, and when you think you're done, double check your work again. Also very clearly indicate all solutions.

NAME: ____

1. (a) Find a positive integer $n < 35$ such that

$$\begin{aligned} n &\equiv 3 \pmod 5, \text{ and} \\ n &\equiv 5 \pmod 7. \end{aligned}$$

(b) Let a and b be integers and $n = pqr$ be a product of three distinct primes. Prove that $a \equiv b \pmod n$ if and only if

$$\begin{aligned} a &\equiv b \pmod p, \text{ and} \\ a &\equiv b \pmod q, \text{ and} \\ a &\equiv b \pmod r. \end{aligned}$$

2. (a) Is the integer $n = 144181$ prime? Why or why not?

(b) Find the prime factorization of the integer $n = 873$.

3. (a) Compute $\log_2(3 \pmod{13})$, i.e., find an integer n such that $2^n \equiv 3 \pmod{13}$.

(b) Is there an integer n such that $3^n \equiv 2 \pmod{13}$?

(c) Find a positive integer $n < 13$ such that $n \equiv 2^{2007} \pmod{13}$.

4. (a) Compute $\gcd(873, 36)$ using any algorithm at all (even being "psychic", i.e., no proof required – just get the right answer).

(b) Find integers x and y such that $11x - 13y = 1$.

5. Nikita's RSA public key is $(n, e) = (35, 7)$.

   (a) Encrypt the number 2 to her.

   (b) For the above public key, figure out what Nikita's RSA private key must be.

Some potentially useful – and some useless – calculations, which you may assume above:

```
sage: print prime_range(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(13,144181)^144180
1
sage: Mod(23,144181)^144180
114019
sage: Mod(7,24)^(-1)
7
sage: Mod(3,35)^7
17

sage: 144*181
26064

sage: a = Mod(2,13); [a^i for i in range(13)]
[1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1]
sage: a = Mod(2,17); [a^i for i in range(17)]
[1, 2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9, 1]
sage: a = Mod(3,17); [a^i for i in range(17)]
[1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]

sage: [2^n for n in range(10)]
[1, 2, 4, 8, 16, 32, 64, 128, 256, 512]
sage: [2007 % k for k in range(1, 20)]
[0, 1, 0, 3, 2, 3, 5, 7, 0, 7, 5, 3, 5, 5, 12, 7, 1, 9, 12]
sage: [35*a for a in range(10)]
[0, 35, 70, 105, 140, 175, 210, 245, 280, 315]

sage: is_prime(873)
False

sage: range?
    range([start,] stop[, step]) -> list of integers

    Return a list containing an arithmetic progression of integers.
    range(i, j) returns [i, i+1, i+2, ..., j-1]; start (!) defaults to 0.
    When step is given, it specifies the increment (or decrement).
    For example, range(4) returns [0, 1, 2, 3].  The end point is omitted!
    These are exactly the valid indices for a list of 4 elements.
```