Discrete Mathematics

Moshe Rosenfeld

Hanoi 2011
moishe@u.washington.edu

Name:

1 Assignment - 10

Due: Tuesday Nov. 29

2 SAGE-Number Theory

This assignment will prepare us for our next topic: Applications of modual arithmetic. We expect you to be familoar with the following terms:

1. **Finite fields** $GF(q)$
2. **Primitive elements in** $GF(q)$
3. **Square roots in** $GF(q)$
4. $a \bmod b$
5. $gcd(a, b) = m \cdot a + n \cdot b$ **(extended gcd)**
6. $a^{-1} \bmod b$
7. **Euler's totiend** $\phi(n)$**.**
8. **Chinese remainder theorem.**
9. **Fermat's little theorem** $a^{p-1} \bmod p = 1$**.**

SAGE exercises

1. **Let** n **be a ten-digit integer (pick your phone number).** m **a second ten-digit number.**

2. **Can you find integers a, b such that $a \cdot n + b \cdot m = 1000$.**

3. **How many times the digit 0 appears in $n!$?**

4. **How many digits does n^m have?**

5. **Let p be the smallest prime $\geq n \cdot m$, find it.**

6. **Can you find an integer k such that $k^2 \bmod p = n$?**

7. **Factor $(mn)^2 + 1$.**

8. **Calculate $m^n \bmod p$.**

2.1 Explorations

1. **How many consecutive integers of the form $a^2 + 6 \cdot b^2, \ a, b > 0$ can you find? Can you formulate a conjcture based on your exploraion?**

2. **11 is a prime number. Find other integers of the form $11 \ldots 1$ that are prime. Can you form a conjecture, theorem based on your experiment?**