Discrete Mathematics
Drill

Moshe Rosenfeld

Hanoi 2011
moishe@u.washington.edu

1 Number Theory

This file will include drills to help you understand the class discussion.
P-P Indicates that this should be done with paper-pencil only, meaning that it is a simple calculation.

1. **P-P** Find all primitive elements in $GF(7)$, in $GF(13)$
2. (SAGE): Find one primitive element in $GF(34296447299)$ (it is a prime number).
3. **P-P** Find $\sqrt{3} \bmod 11$.
4. **P-P** Find the roots of $x^2 + 3x + 7$ in $GF(19)$ and factor it.
5. **P-P** Find $\sqrt{53} \bmod 143$
6. **P-P** Calculate $3^{57} \bmod 24$.
7. (SAGE): 413138881 is not prime. Check whether 7 is a "composite-witness." Find an integer $k < 10$ which is a composite witness.
8. **P-P** Find all $\sqrt{58} \bmod 77$.
9. (SAGE:) $n = 230174582312854321522280751140129890849 0$ is a quadratic residue mod $2025355709778494687384806231977593978636 11$ $(= k)$. Two square roots of $n \bmod k$ are $1433228142575501917246866153449361844214 37$ and $3806580988275895075227659976771293246 73$.
   - Verify that indeed both are square roots of n.
   - Use the square roots to factor k.
   - Note: **after** you use what we learned and factored k you can use the factor() method in SAGE and compare the results. SAGE can factor integers with 42 digits quite fast.