# MATH 3320, HOMEWORK #5

DUE FRIDAY, SEPTEMBER 28

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

These are hints based on questions answered during the homework session on Wednesday September 26.

**1.** For each integer $n \geq 0$, define the *Fermat number*

$$F_n = 2^{2^n} + 1.$$

(a) (5 points) By induction, prove that

$$F_0 F_1 \cdots F_{n-1} = F_n - 2$$

for all $n \geq 1$.

(b) (5 points) Using part (a), deduce that $\gcd(F_n, F_m) = 1$ for distinct $n$ and $m$.

(c) (10 points) Use part (b) to give a proof that there are infinitely many prime numbers.

**2.** Let $p$ be an odd prime.

(a) (10 points) Prove that there is at least one primitive root modulo $p^2$. (Hint: If $a$ and $b$ have order $m$ and $n$ respectively, such that $\gcd(m, n) = 1$, what is the order of $ab$?)

**Hint:** (Covered in class in one of the sections) Let $g$ be an element of order $p-1$ modulo $p$. If $g$ does have order $p(p-1)$, done. If not, the order is $p-1$. Look at $g+p$.

Using the hint about the orders. Suppose the order of $g$ is $p-1$. Check the order of $1+p$, or any $1+kp$ with $k$ prime to $p$.

(b) (10 points) Prove that for any $n \in \mathbf{N}$, there is at least one primitive root modulo $p^n$.

**Hint:** Any element in $\mathbb{Z}_{p^e}$ can be written as $k_0 + k_1 p + \cdots + k_{e-1} p^{e-1}$ with unique $k_i \in \mathbb{Z}_p$. Do an induction on the $e$ of $p^e$. You might check the order of $(1+p)$ $(mod\ p^{e+1})$, and find an element of order $(p-1)$ using the induction hypothesis.

(c) (5 points) Find an explicit primitive root modulo 343.

**Hint:** $343 = 7^3$. Try to use the previous parts of the problem to build a primitive element modulo 7, then $7^2$ and then $7^3$. Or try to find elements of orders prime to each other and multiply.

**3.** (30 points) In terms of the prime factorization of $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \in \mathbf{N}$ (where $p_i$'s are distinct primes and $e_i \in \mathbf{N}$), characterize the integers $m \in \mathbf{N}$ for which there exists a primitive root modulo $m$. (Hint: For example, $m = 8$ does *not* have a primitive root modulo $m$. Why is this the case? What about prime powers? Products of prime powers?)

**Hint:** Use CRT to reduce the question to similar ones for the individual $\mathbb{Z}_{p_i^{r_i}}$. If $a$ has order $x$, $b$ has order $y$, and $(x, y) = d > 1$, what is the order of $ab$?

**4.** A computer is recommended for this problem, but you don't need to get too sophisticated; just be able to do modular arithmetic. I suggest using `Sage` (a.k.a. `Sagemath`) (or its online analogue: `CoCalc`), as it has a lot of built-in number-theoretic functions[1]. (To get full credit, remember to describe describe *how* you got the answers, not just state the answers themselves.)
**Further Hint:** I posted some simple minded programs in Mathematica which you can adapt to your favorite programming language. CoCalc, which used to be SageMathCloud is available for free. Documentation/simple commands useful for elementary number theory can be found at `http://doc.sagemath.org/html/en/constructions/number_theory.html`

(a) (5 points) You and Bob wish to agree on a secret key using the Diffie–Hellman key exchange. Bob announces that $p = 2141$ and $g = 11$. Bob secretly chooses a number $n < p$ and tells you that $g^n \equiv 2114 \pmod{p}$. You choose the random number $m = 1234$. What is the secret key?

(b) (10 points) You discover that Bob is selling out your secrets to Alice, using the Diffie–Hellman key exchange. You see Alice and Bob agree on a secret key, choosing $p = 101$ and $g = 7$. Alice chooses a random number $n$ and tells Bob that $g^n \equiv 48 \pmod{p}$. Bob chooses a random number $m$ and tells Alice that $g^m \equiv 21 \pmod{p}$. Crack their code using brute force: What is the secret key that Alice and Bob agree upon? What is $n$? What is $m$?

**5.** (Extra credit) Each of the following messages has been encrypted using a simple substitution cipher (i.e. one letter corresponds to another letter). Decrypt them. (I suggest frequency analysis first and foremost, i.e. mapping common letters in English to common letters in the ciphertext.)

There are four cryptograms in the file at

`http://pi.math.cornell.edu/~web3320/HWK/cryptograms.txt`

Each subsequent one has a little bit of a twist. Cryptograms (a) and (b) are worth (2 points) each, while (c) and (d) are worth (3 points) each, for (10 points) total.

In addition to writing the plaintext (with formatting restored), include a brief description of how you decoded the messages, including relevant code if you used a computer. (Using a computer is highly recommended.)

[1] `https://wiki.sagemath.org/quickref?action=AttachFile&do=get&target=quickref-nt.pdf`