Study guide

- (§14) Know the definition of a Mersenne prime.
- (§14) Be able to prove: if $2^p - 1$ is prime, then p is prime as well.
- (§15) What is the link between Mersenne primes and (even) perfect numbers?
- (§15) Understand the importance of *multiplicativity* in the study of perfect numbers.
- (§16) How can you use the *successive squaring* technique to quickly compute modular powers (by hand if needed)?

1. (Textbook 14.1)
   Prove that if $a \geq 2$ and $n \geq 1$ are integers, and $a^n + 1$ is prime, then n is a power of 2.

2. (Textbook 14.2, on Fermat primes)
   Let $F_k = 2^{2^k} + 1$. For example, $F_1 = 5, F_2 = 17, F_3 = 257$, and $F_4 = 65537$. Fermat thought that all the F_k 's might be prime, but Euler showed in 1732 that F_5 factors as $641 \cdot 6700417$, and in 1880 Landry showed that F_6 is composite. Primes of the form F_k are called Fermat primes. Show that if $k \neq m$, then the numbers F_k and F_m have no common factors; that is, show that $\gcd(F_k, F_m) = 1$. [Hint. If $k > m$, show that F_m divides $F_k - 2$.]

3. (Textbook 14.3, on primes of the form $\frac{1}{2}(3^n - 1)$)
   The numbers $3^n - 1$ are never prime (if $n \geq 2$), since they are always even. However, it sometimes happens that $(3^n - 1)/2$ is prime. For example, $\left(3^3 - 1\right)/2 = 13$ is prime.

   (a) Find another prime of the form $(3^n - 1)/2$.

   (b) If n is even, show that $(3^n - 1)/2$ is always divisible by 4 , so it can never be prime.

   (c) Use a similar argument to show that if n is a multiple of 5 then $(3^n - 1)/2$ is never a prime.

   (d) Do you think that there are infinitely many primes of the form $(3^n - 1)/2$?

4. (Textbook 15.3, on the impossibility of certain odd perfect numbers)

   (a) Show that a power of 3 can never be a perfect number.

   (b) More generally, if p is an odd prime, show that a power p^k can never be a perfect number.

   (c) Show that a number of the form $3^i \cdot 5^j$ can never be a perfect number.

   (d) More generally, if p is an odd prime number greater than 3 , show that the product $3^i p^j$ can never be a perfect number.

   (e) Even more generally, show that if p and q are distinct odd primes, then a number of the form $q^i p^j$ can never be a perfect number.

5. (Textbook 15.8, on "amicable numbers")
   The Greeks called two numbers m and n an amicable pair if the sum of the proper divisors of m equals n and simultaneously the sum of the proper divisors of n equals m. (The proper divisors of a number n are all divisors of n excluding n itself.) The first amicable pair, and the only one (as far as we know) that was known in ancient Greece, is the pair $(220, 284)$. This pair is amicable since

$$284 = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 \quad \text{(divisors of 220)}$$
$$220 = 1 + 2 + 4 + 71 + 142 \quad \text{(divisors of 284).}$$

(a) Show that m and n form an amicable pair if and only if $\sigma(n)$ and $\sigma(m)$ both equal $n+m$.

(b) Verify that each of the following pairs is an amicable pair of numbers.

$$(220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368)$$
$$(10744, 10856), (12285, 14595)$$

(c) There is a rule for generating amicable numbers, although it does not generate all of them. This rule was first discovered by Abu-1-Hasan Thabit ben Korrah around the ninth century and later rediscovered by many others, including Fermat and Descartes. The rule says to look at the three numbers

$$p = 3 \cdot 2^{e-1} - 1$$
$$q = 2p + 1 = 3 \cdot 2^e - 1$$
$$r = (p+1)(q+1) - 1 = 9 \cdot 2^{2e-1} - 1$$

If all of p, q, and r happen to be odd primes, then $m = 2^e pq$ and $n = 2^e r$ are amicable. Prove that the method of Thabit ben Korrah gives amicable pairs.

(d) Taking $e = 2$ in Thabit ben Korrah's method gives the pair $(220, 284)$. Use his method to find a second pair. If you have access to a computer that will do factorizations for you, try to use Thabit ben Korrah's method to find additional amicable pairs.

So we also get another amicable pair from $e = 7$, but then not another for awhile.

6. Evaluate the following using the method of successive squaring. Try to do as much by hand as possible, but use a calcualtor as needed (look for ways to make your calculations easier where you can). Note that on exams, I will often provide a multiplication table for modular arithmetic if the modulus is larger than 20 or so, so you won't have to do anything quite this complicated by hand under time pressure.

(a) The remainder when 2^{25} is divided by 29.

(b) The last two digits of 29^{72}.

(c) The remainder when 49^{37} is divided by 101.