M328K – Rusin – HW6 – ANSWERS

1. Suppose a and b are positive integers. Show that if $a^3|b^2$ then $a|b$. Can we also conclude that $a|b$ if instead we are instead told that $a^2|b^3$?

ANSWER: Write the prime factorizations of a and b as $a = \prod p^{e_p}$ and $b = \prod p^{f_p}$ respectively. Here the products run over *all* primes, with the exponents e_p and f_p being zero for almost all primes (e.g. $9 = 2^0 3^2 5^0 \ldots$). Then the assertion that $a^3|b^2$ can be restated as the fact that for every prime p, $3e_p \leq 2f_p$ (using here the Fundamental Theorem of Arithmetic). But then each e_p is no larger than $\frac{2}{3}f_p$, which in turn is less than or equal to f_p itself. Then since $e_p \leq f_p$ for every p, it follows that $a|b$.

With the exponents the other way around the statement is false, e.g. $8^2|4^3$ but obviously $8 \not| 4$.

2. For each positive integer n, let us write M_n for the nth Mersenne number, that is, $M_n = 2^n - 1$.

(a) Show that whenever $k|n$ then $M_k|M_n$.

(b) Show that if d divides two Mersenne numbers M_k and M_n with $k < n$, then it divides M_{n-k}.

I won't assign it but you might accept the following challenge: show that $\gcd(M_r, M_s) = M_{\gcd(r,s)}$.

ANSWER: For part (a), if $n = kd$ then $2^n - 1 = (2^k)^d - 1$. But $X - 1$ divides $X^d - 1$ for every X, and when $X = 2^k$ this means $M_k|M_n$.

For part (b) note that d would certainly divide $M_n - M_k = 2^n - 2^k = 2^k \cdot (2^{n-k} - 1)$. But the Mersenne numbers are all odd, so their divisors d are as well, i.e. they are coprime to 2 (and its powers). Thus d would have to divide the other factor $2^{n-k} - 1 = M_{n-k}$. (We can also reverse the reasoning: if d divides both M_{n-k} and M_k then it divides M_n. Thus any pair among these three Mersenne numbers has the same gcd.)

For the challenge note that if $n = kq + r$, then by applying part (b) q times we conclude $\gcd(M_n, M_k) = \gcd(M_k, M_r)$. Thus we can carry out the very steps used in the Euclidean Algorithm, always finding pairs k_i, n_i such that $\gcd(M_{n_i}, M_{k_i}) = \gcd(M_n, M_k)$, terminating only when $k_i|n_i$, at which point we know $k_i = \gcd(n, k)$.

3. Suppose a and b are coprime integers, and that one of them is even and the other is odd. Show that $a - b$ and $a^3 + b^3$ are also coprime.

ANSWER: If these two integers have a common factor d then, modulo d, we have both $a \equiv b$ and $a^3 \equiv -b^3$. But of course if $a \equiv b$ then $a^3 \equiv b^3$, so by transitivity we would also have $b^3 \equiv -b^3$, or $2b^3 \equiv 0$. Now, since a and b have different parity, it follows that $a - b$ is odd, and so its divisor d must be as well. Thus 2 has an inverse mod d and we conclude $b^3 \equiv 0$.

In particular, if p is any prime divisor of d, then p divides b^3 and hence b itself. But since $p|d|(a - b)$, that would mean p also divides a, which contradicts the assumption that a and b are coprime. So there is no such p, which means $d = 1$, i.e. $a - b$ and $a^3 + b^3$ are coprime.

4. *Twin primes* are primes p and q which differ by 2. For example 11 and 13 are twin primes. Prove that there are infinitely many primes which are NOT part of a twin-prime pair.

ANSWER: See answers to Homework 5.

5. A vague but important question is: how far apart are the primes? That is, if we number the primes in order,

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \quad \ldots$$

then can we estimate how big the gap $p_{n+1} - p_n$ is, compared to p_n itself? Obviously the size of that gap will vary: for example, if it turns out that the Twin Prime Conjecture is true, then there will be infinitely many values of n for which $p_{n+1} - p_n$ is just 2. On the other hand, there can be arbitrarily long gaps between the primes (see Theorem 3.5). But the size of the gap from p_n to p_{n+1} can be bounded by the size of p_n:

(a) Find Bertrand's Conjecture in the book. (This conjecture is known to be true.) Use it to show that $p_{n+1} - p_n < p_n$,

(b) Find Legendre's Conjecture in the book. (This conjecture is NOT yet known to be true.) Show that if it's true, then $p_{n+1} - p_n < 4\sqrt{p_n} + 2$.

(Researchers think that the gaps are *never* even close to the sizes shown in this problem; it's probably true that the gaps are never more than roughly $\log(p_n)^2$.)

ANSWER: Bertrand's Conjecture states (as a theorem) that for every integer $k > 1$ there is a prime between k and $2k$. Taking $k = p_n$ shows us that the next prime, p_{n+1} is less than $2p_n$, so that $p_{n+1} - p_n < p_n$, as desired.

If Legendre's Conjecture turns out to be true, then we would argue as follows: let k^2 be the largest perfect square which is less than p_n. The Conjecture would guarantee that there is another prime between $(k+1)^2$ and $(k+2)^2$, and it can't be as large as $(k+2)^2 - 1 = (k+1)(k+3)$ because that number is composite! So the gap betweenp_n and p_{n+1} would be smaller than the gap between k^2 and $(k+2)^2$; more precisely we would have $p_{n+1} - p_n \leq [(k+2)^2 - 2] - [k^2 + 1] = 4k + 1 < 4\sqrt{p_n} + 1$.