WRITTEN HW #3 SOLUTIONS

(1) (10 points) Suppose that $\gcd(q, a) = 1$. Dirichlet's Theorem (which we stated but never proved) says that there are infinitely many primes of the form $qk+a$, where $k \in \mathbb{Z}$. On the other hand, show that there are infinitely many values of k such that $qk + a > 0$ and $qk + a$ is composite.

Solution. Let us look at the values of $qk + 1$, where $\gcd(q, a) = 1$. Let p be some prime which does not divide q or a. Consider the values $q + a, 2q + a, 3q + a, \ldots, (p-1)q + a$. Since p doesn't divide q or a, one of these values is a multiple of p; assume it is $nq + a$. Then for $k = pm + n$, $qk + a = (pm + n)q + a = pmq + nq + a$ is divisible by p, and thus can be prime for at most one value of m. The rest of the numbers of this form must be composite. $\square$

(2) (10 points) Recall that we defined the binomial coefficient n choose m to equal

$$\binom{n}{m} = \frac{n!}{m!(n-m)!},$$

and that in the first homework assignment we saw this was equal to an integer. Let p be a prime, and let $0 < i < p$. Show that the power of p appearing in the factorization of $\binom{p}{i}$ is 1; ie, show that $p \,||\, \binom{p}{i}$.

Solution. Recall that if $0 < i < p$, then $p \nmid i$, so p does not appear in the prime factorization of i. Since $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, if we write $p! = p(p-1)\ldots(2)(1)$, we see that p appears in only one factor in the numerator of $\binom{p}{i}$, so $p \parallel p!$. Looking at the denominator, as long as $0 < i < p$, then p does not divide either $i!$ or $(n-i)!$, since both $i, n - i < p$. Hence p does not divide the denominator, so $p \parallel \binom{p}{i}$. $\square$

(3) (10 points) Let p be a prime, and let n be a positive integer. Find an expression for the power of p in the factorization of $\operatorname{lcm}(1, 2, 3, \ldots, n)$, and prove that your answer is correct.

Solution. First, we claim that if $n_1 = p_1^{e_{11}} \ldots p_k^{e_{1k}}, n_2 = p_1^{e_{21}} \ldots p_k^{e_{2k}}, \ldots, n_r = p_1^{e_{r1}} \ldots p_k^{e_{rk}}$, then

$$\operatorname{lcm}(n_1, \ldots, n_r) = p_1^{m_1} \ldots p_k^{m_k},$$

where $m_i = \max(e_{1i}, e_{2i}, \ldots, e_{ri})$ is the maximum of all the exponents of the ith prime p_i in the factorizations of $n_1, \ldots, n_r$. Indeed, this follows from the fact that $b \mid a$ if and only if the exponent of each prime p appearing in the factorization of b divides the exponent of p in the factorization of a.

Therefore, for an arbitrary prime p, the power of p in the factorization of $L = \text{lcm}(1, 2, 3, \ldots, n)$ is the highest power of p less than or equal to n. Let p^k be the highest power. On the other hand, We want $p^k \le n < p^{k+1}$, or equivalently $k \le \log_p(n) < k + 1$. Hence the expression we are looking for is $\lfloor \log_p n \rfloor$. $\square$

(4) (10 points) Let $a, b > 1$ be two integers which do not have all the same prime factors. (For instance, $a = 6, b = 24$ would not satisfy this property, since their prime factors are the same; namely, $2, 3$, whereas $a = 10, b = 8$ would, since $5 \mid a, 5 \nmid b$.) Show that $\log_a b$ is an irrational number.

Solution. First, notice that because $b > 1$, $\log_a b > 0$. Suppose $\log_a b$ were rational; say of the form m/n, where $m, n > 0$. Then

$$a^{m/n} = b, \text{ or } a^m = b^n.$$

However, if $p \mid a, p \nmid b$, then p divides the left hand side but not the right hand side, a contradiction. Similarly if $p \mid b, p \nmid a$. $\square$

(5) (10 points) Show that there are infinitely many prime numbers in the form $8k + 5$ or $8k + 7$.

Solution. (In this problem, you are not supposed to use Dirichlet's Theorem.) Suppose there were only finitely many primes of form $8k+5$ or $8k+7$; call them $p_1, \ldots, p_k$. Let $N = 8p_1 \ldots p_k - 1$. Notice that $p_i \nmid N$ for all $1 \le i \le k$, since $p_i \mid (8p_1 \ldots p_k)$, but $p_i \nmid -1$. Also, N is not even. Therefore, N is a product of primes of form $8k+1$ and $8k+3$. However, notice that a product of numbers of these two forms is always of form $8k + 1$ or $8k + 3$. Indeed, using congruence notation, if $a, b \equiv 1 \text{ or } 3 \bmod 8$, then $ab \equiv 1, 3, 3 \cdot 3 \equiv 1, 3, 1 \bmod 8$. But then this means $N \equiv 1, 3 \bmod 8$, which is evidently impossible because the definition of N shows that $N \equiv 7 \bmod 8$. $\square$