HOMEWORK ASSIGNMENT #3 SOLUTIONS

(1) Show that there are infinitely many primes of the form $6k+5$. (Obviously, you are not supposed to cite Dirichlet's Theorem or anything of that sort. You should be using the methods in Euclid's proof for the infinitude of prime numbers and the modification of the method for primes of the form $4k+3$.)

Solution. Suppose there are only finitely many primes of the form $6k+5$; say $p_1, \ldots, p_n$. Let $N = 6p_1 \ldots p_n - 1$. First, notice that this is a number of the form $6k+5$ bigger than any individual p_i. Next, notice no p_i divides N, nor do $2, 3$ divide N.

Every prime number is either of the form $6k+1, 6k+5$, or $2, 3$. Indeed, there are no primes of the form $6k$, since 2 is a proper divisor of all such positive integers, the only prime of the form $6k+2$ is 2, the only prime of the form $6k+3$ is 3, and there are no primes of the form $6k+4$, since again 2 is a proper divisor of all such positive integers. Since $2, 3$, no p_i divides N, this means that N must be a product of only primes of the form $6k+1$.

However, this is impossible, because a product of numbers all of the form $6k+1$ is still $6k+1$. Indeed, if $m, n \equiv 1 \mod 6$, then $mn \equiv 1 \mod 6$. □

(2) Prove the following generalization of the fact that $\sqrt{2}$ is irrational: if k is a positive integer, and n is not a perfect kth-power (ie, if $\sqrt[k]{n}$ is not an integer), then $\sqrt[k]{n}$ is irrational.

Solution. Suppose $\sqrt{k}[n]$ were rational, say equal to a/b, where $\gcd(a,b) = 1, n \neq 0, m, n > 0$. (If n is negative, which is possible if k is odd, replace n with $-n$.) Then $n = a^k/b^k$, or $nb^k = a^k$. Because n is not a perfect k-th power, there is some prime p dividing n such that the exponent of p in the factorization of n is not divisible by k. But then $nb^k = a^k$ is impossible, because the exponent of p in the factorization of nb^k is not divisible by k, but the exponent of p in the factorization of a^k is divisible by k, a contradiction. □

(3) Let n be a positive integer and let N be the least common multiple of $1, 2, \ldots, n$. Show that the sum of the exponents appearing in the prime factorization of N is always less than n.

Solution. We prove this statement by induction. First, notice that when $n = 1$ (or $n = 2$, doesn't matter), the statement is true. (If you are wondering what this statement means when $n = 1$, the LCM is equal to 1, and the sum of the exponents in the prime factorization is 0, since $1 = 2^0 3^0 \ldots$.)

Suppose we have proven the statement for n, and want to prove it for $n+1$. Let $N = \operatorname{lcm}(1, 2, \ldots, n), N' = \operatorname{lcm}(1, 2, \ldots, n+1)$, and let e be the sum of the exponents of the factorization of N, and e' the same sum for N'. We will show that $e' \leq e + 1$. (Obviously $e \leq e'$, since $N \mid N'$.) There are three separate cases to analyze.

First, if $n+1=p$ is prime, then p is coprime to all of $1,2,\ldots,n$, hence coprime to N, so $N'=p\cdot N$. The one sees that $e'=e+1$.

Second, if $n+1=p^e$, for some prime p, $e>1$, then the prime power p^{e-1} is amongst the numbers $2,3,\ldots,n$, since $p^{e-1}\leq p^e/2<n+1$. This means that the exponent of p in the factorization of N is $e-1$, because $p^{e-1}\mid N$, but $p^e\nmid N$ since $n<p^e$. Then we see that $N'=pN$, because $\gcd(p^e,N)=p^{e-1}$, so that $N'=\operatorname{lcm}(p^e,N)=p^eN/\gcd(p^e,N)=pN$. Again, we have $e'=e+1$.

Finally, suppose $n+1$ is divisible by two distinct primes q_1,q_2. Let p be any prime dividing $n+1$, and let p^i be the power of p appearing in the factorization of $n+1$. Let $n+1=p^id$. Then $1<d<n+1$, because $n+1$ is divisible by two distinct primes. Therefore p^i is amongst the numbers $2,3,\ldots,n$. So the prime power p^i already divides N. Since this is true of all prime powers dividing $n+1$, this means that $\gcd(n+1,N)=n+1$, or alternatively, $N=N'$, which means $e=e'$.

Since these three cases cover all possibilities for $n+1$, we are done. □

(4) Recall that for integers n,m satisfying $0\leq m\leq n$, the binomial coefficient $\binom{n}{m}$ is defined to be the expression

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

For instance, $\binom{4}{2}=4!/(2!2!)=24/4=6$, while $\binom{7}{0}=7!/(7!0!)=1$ and $\binom{5}{3}=5!/(3!2!)=120/12=10$. This number is equal to the number of ways of choosing m objects from a set of n objects, and so is an integer. If p is a prime and $1<k<p$, show that $\binom{p}{k}$ is divisible by p.

Solution. We have

$$\binom{p}{k}=\frac{p!}{(p-k)!k!}.$$

First, notice that p divides the numerator. However, p does not divide the denominator, because every number in the two products in the denominator is less than p. Since we are told $\binom{p}{k}$ is an integer, this implies that p divides the integer $\binom{p}{k}$, because the factor of p in the numerator is not cancelled out when reducing $\dfrac{p!}{(p-k)!k!}$ to an integer. □

(5) Recall that we can test a positive integer for divisibility by 2 if its last digit is even, and for divisibility by 4 by checking if its last two digits form a number divisible by 4. Show that we can test a positive integer for divisibility by 2^k by checking if the number formed by its last k digits is divisible by 2^k.

Solution. Let n be a positive integer we want to test for divisibility by 2^k. Let b be the number formed by the last k digits of n, and let a be the number formed by the remaining digits. For example, if $k=3, n=12434$, then $a=12, b=434$. Then $n=10^ka+b$. Since $2^k\mid 10^k$, this implies that

$$n=10^ka+b\equiv b \mod 2^k.$$

Since $2^k\mid n$ if and only if $n\equiv 0 \mod 2^k$, this implies that one of n,b is divisible by 2^k whenever the other is. □

(6) Find all solutions (there may be none) of the following congruences. Be sure to explain why your answer is correct.

(a) $5x \equiv 7 \mod 12$.
(b) $21x \equiv 13 \mod 105$.
(c) $9x \equiv 6 \mod 15$.
(d) $x^2 \equiv 1 \mod 11$.
(e) $x^2 \equiv 1 \mod 8$.

Solution.

(a) Since $\gcd(5, 12) = 1$, $5x \equiv 7 \mod 12$ has exactly one solution mod 12. Trial and error, or any other method you like, yields $x \equiv 11 \mod 12$ as that solution.
(b) Since $\gcd(21, 105) = 21$, but $21 \nmid 13$, the congruence $21x \equiv 13 \mod 105$ has no solutions.
(c) The number 3 divides every number in the congruence $9x \equiv 6 \mod 15$, so this is equivalent to $3x \equiv 2 \mod 5$. Since $\gcd(3, 5) = 1$, this has exactly one solution mod 5, which trial and error, or any other method you like, yields $x \equiv 4 \mod 5$.
(d) We saw that $x^2 \equiv 1 \mod p$ has exactly two solutions, $x \equiv \pm 1 \mod p$, whenever p is prime. So $x \equiv 1, 10 \mod 11$ are the two solutions to $x^2 \equiv 1 \mod 11$. Alternately, you can use trial and error.
(e) Trial and error shows that $x \equiv 1, 3, 5, 7 \mod 8$ are all the solutions. □

(7) Find last digit of the following numbers. The work you show should not assume the use of a calculator or other computational device at any point.

(a) 7^{7143},
(b) $23! + 19! + 15! + 11! + 7! + 3!$,
(c) $2 \upuparrows n$, for $n \geq 3$, where $a \upuparrows n$ means a power tower of a with size n: for instance, $2 \upuparrows 3 = 2^{2^2} = 2^4$, while $2 \upuparrows 4 = 2^{2^{2^2}} = 2^{2^4} = 2^{16}$. (Remember that towers of exponentials are evaluated from the top down, not the bottom up, so for instance $3^{3^3} = 3^{27}$, not $(3^3)^3 = 27^3$, which is a much smaller number than 3^{27}.

Solution. Finding the last digit is equivalent to finding the remainder mod 10, so we will do that.

(a) One sees that $7^2 \equiv 9 \mod 10$, so $7^4 \equiv 9^2 \equiv 1 \mod 10$. The remainder when we divide 7143 by 4 is 3, so $7^{7143} \equiv 7^3 \equiv 3 \mod 10$.
(b) The numbers $7!, 11!, 15!, 19!, 23!$ all end in 0, since they are all divisible by both $5, 2$. So the number in question has last digit equal to the last digit of $3!$, which is 6.
(c) First notice that $2 \upuparrows n = 2^{2 \upuparrows (n-1)}$. For $n \geq 3$, this exponent is always divisible by 4, since $2 \upuparrows (n-1) = 2^{2 \upuparrows (n-2)}$, and $2 \upuparrows (n-2) \geq 2$ for $n \geq 3$. We now claim that $2^k \equiv 6 \mod 10$ if $4 \mid k$. Indeed, $2^4 \equiv 6 \mod 10$, and $6 \cdot 6 \equiv 6 \mod 10$, so any number of products of 2^4 together; that is, any power of 2^4, has last digit 6. □