Math 124 Problem Set 1

1. First, we show that the binomial coefficient is an integer.

Claim: For fixed n and $0 \leq k \leq n$, $\binom{n}{k}$ is an integer.

Proof. By induction. Clearly $\binom{1}{0} = \binom{1}{1} = 1$. Suppose that $\binom{n}{k}$ is an integer for $0 \leq k \leq n$. Now $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ and for $0 \leq i \leq n-1$

$$\binom{n}{i} + \binom{n}{i+1} = \frac{n!}{i!(n-i-1)!}\left(\frac{1}{n-i} + \frac{1}{i+1}\right) = \frac{(n+1)!}{(i+1)!(n-i)!} = \binom{n+1}{i+1},$$

which by the inductive hypothesis is the sum of two integers. This proves the claim.

Since p is prime, it is sufficient to show that there is no factor of p in the denominator. By assumption, $r < p$ so $r!$ does not contain a factor of p. Similarly, $1 \leq r$ implies that $p - r \leq p - 1 < p$, so $(p-r)!$ also contains no factor of p.

2. $gcd(15, 35) = gcd(35, 15) = gcd(5, 15) = gcd(15, 5) = gcd(0, 5) = \mathbf{5}$;

$gcd(247, 299) = gcd(247, 52) = gcd(52, 39) = gcd(39, 13) = gcd(13, 0) = \mathbf{13}$;

$gcd(51, 897) = gcd(51, 30) = gcd(30, 21) = gcd(21, 9) = gcd(9, 3) = gcd(3, 0) = \mathbf{3}$;

$gcd(136, 304) = gcd(136, 32) = gcd(32, 8) = gcd(8, 0) = \mathbf{8}$;

3a. The base case is trivial. Suppose that $1 + \ldots + n = \frac{n(n+1)}{2}$ for some n. Then

$$1 + \ldots + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

as desired.

3b. If n is even we may the group the terms as $(1-2) + (3-4) + \ldots + (n-1-n)$, yielding the formula $-\frac{n}{2}$. Similarly, if n is odd we have $1 + (-2+3) + (-4+5) + \ldots + (-(n-1)+n)$, which gives the formula $1 + \frac{n-1}{2} = \frac{n+1}{2}$.

Therefore the general formula is $(-1)^{n+1}\lceil \frac{n}{2} \rceil$.

4. We can run $precprime(2001)$ in PARI, which gives 1999.

5. The Euclidean Algorithm gives us:

$2261 = 1275 \cdot 1 + 986$; $1275 = 986 \cdot 1 + 289$; $986 = 289 \cdot 3 + 119$; $289 = 119 \cdot 2 + 51$; $119 = 51 \cdot 2 + 17$, so

$$\begin{aligned} 17 &= 119 - 51 \cdot 2 = (986 - 289 \cdot 3) - (289 - 119 \cdot 2) \cdot 2 \\ &= 986 - (1275 - 986) \cdot 3 - (1275 - 986) \cdot 2 + (986 - 289 \cdot 3) \cdot 4 \\ &= 1275 \cdot -5 + 986 \cdot 10 + 289 \cdot -12 = 1275 \cdot -17 + 986 \cdot 22 \\ &= \mathbf{22} \cdot 2261 - \mathbf{39} \cdot 1275. \end{aligned}$$

6. $factor(2005)$ yields 2005 = 5 x 401.

7. $for(i = 1, 5, print(\text{“}HelloKitty\text{”}))$

8. A necessary condition is that the polynomial $f(x)$ is irreducible over $\mathbf{Z}$; this would include the condition that the gcd of the coefficients is 1. Certainly if f is reducible then each factor could take the value 1 only a finite number of times (hence f can be prime only at a finite number of integers). In the case where $deg(f) = 1$ Dirichlet's theorem confirms that $ax + b$ will take infinitely many prime values if $(a, b) = 1$, and in class the conjecture for $f(x) = x^2 + 1$ was presented.

To test a given f, we could use the following PARI code:

$$f0(n) = for(i = 0, n, if(isprime(f(n-i)), return(n-i)));$$

and then try $f0(n)$ for large values of n. I tried this for some cyclotomic polynomials: n^2+n+1, n^2+1, $(n^5-1)/(n-1)$ and also for n^3-n+1 for n up to 10 billion. All returned values close to the input. For example, for n^3-n+1 the call to $f0(1000000000)$ gave 999999986. This suggests that for these polynomials the conjecture may be true, although it sheds little light on the general case of irreducible polynomials.

9. We can show that the Euclidean Algorithm on m, n takes $O(|max(m, n)|)$ modular operations, where $|max(m, n)|$ is the number of binary digits of $max(m, n)$. This is done by noting that if we proceed from (x, y) to $(y, x(mod\ y)$ (where $x \geq y$) then $x(mod\ y) \leq x/2$. For if $2y > x \geq y$ then $x(mod\ y) = x - y$. Combining this with $y > x/2$ yields $x(mod\ y) \leq x/2$. Similarly, if $x > 2y$ then $x/2 > y > x(mod\ y)$. Therefore every two steps the original binary representation of x is reduced by one digit.

Now since $10 < 2^4$, a 2000 digit number has fewer than 8000 bits, so PARI can easily compute the gcd of two such numbers.

10. First we note that all odd integers must be congruent to 1, 3 or 5 modulo 6, and if $x \equiv 3(mod\ 6)$ then $3|x$. Therefore all odd primes (except 3) must be congruent to 1 or -1 modulo 6. Next we note that if $p, q \equiv 1(mod\ 6)$ then $pq \equiv 1(mod\ 6)$. Therefore if $n \equiv -1(mod\ 6)$ then n must have a prime factor $p \equiv -1(mod\ 6)$ (3 has no inverse).

Let $T = \{p : p\ prime,\ p \equiv -1(mod\ 6)\}$. Suppose T is finite. Since T is nonempty ($5 \in T$), we can define S_0, the product of elements in T. Now consider $S = 6S_0 - 1$. Since $S \equiv -1(mod\ 6)$, $q|S$ for some $q \in T$. But for all $p \in T$, $S \equiv -1(mod\ p)$, a contradiction. Therefore T is infinite.

11a. We can define a function which computes $\pi(n)$:

$$f(n) = s = 0; for(i = 1, n, if(isprime(i), s++)); s$$

which gives $\pi(2001) = 303$.

11b. For $x = 2001$, $x/log(x) \approx 263$, so the values differ by about 40.