Math 467 Factorization and Primality Testing, Fall 2023, Solutions 1

1. Let $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$ with $0 \le m \le n$. The binomial coefficient $\binom{n}{m}$ is defined inductively by

$$\binom{0}{0} = 1, \quad \binom{n}{-1} = 0, \quad \binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

(i) Prove that $\binom{n}{m} \in \mathbb{N}$. We have $\binom{1}{m} = \binom{0}{m-1} + \binom{0}{m} = 1$ when $m = 0$ or 1 and is 0 otherwise. Then the general result follows immediately by induction on n.

(ii) Prove that if p is a prime and $1 \le m \le p-1$, then $p|\binom{p}{m}$. Clearly the binomial coefficients are uniquely determined. But $\binom{n}{m} = \frac{n!}{(n-m)!m!}$ also satisfies the defining relationship. Then $\binom{p}{m}(p-m)!m! = p!$. This is divisible by p, but $(p-m)!m!$ is not.

2. Prove that no polynomial $f(x)$ of degree at least 1 with integral coefficients can be prime for every positive integer x.

We argue by contradiction. Let $p = f(1)$. Now let $x = 1 + yp$ where y will be taken to be so large that $f(x) > p$. In particular $f(x)$ will be a prime differing from p. But, for example by expanding out $f(1+yp)$, we see that $f(1+yp) = f(1) + pk = p(k+1)$ for some integer k but p will not divide $f(x)$.

3. If $2^n + 1$ is an odd prime for some integer n, prove that n is a power of 2.

Suppose on the contrary that $n = pm$ for some odd prime p. Then we can use the identity

$$x^p + 1 = (x+1)(x^{p-1} - x^{p-2} + \cdots - x + 1)$$

with $x = 2^m$, so that

$$2^n + 1 = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + \cdots - 2^m + 1)$$

and each of the factors on the right exceeds 1.

4. Prove that every positive integer is uniquely expressible in the form $2^{j_0} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_m}$ where $m \ge 0$ and $0 \le j_0 < j_1 < j_2 < \cdots < j_m$.

Existence is an easy induction on observing that every n is of the form $2m$ or $2m+1$ for some m. Uniqueness follows from the fact that $2^{j_0} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_{m-1}} < 2^{j_m}$ and so j_m is uniquely determined by $n/2 < 2^{j_m} \le n$.

5. Prove that there are no positive integers a, b, n with $n > 1$ such that $(a^n - b^n)|(a^n + b^n)$.

Suppose it is possible. Then we may suppose further that (1) $a > b$ and (2) it would be possible with a and b having no common factor. Also $a^n - b^n$ will divide both $a^n + b^n \pm (a^n - b^n) = 2a^n$ and $2b * n$. But since a and b have no common factor we have (3) $a^n - b^n = 1$ or 2. Since $a > b$ we have $a \ge b + 1$ and so $a^n \ge (b+1)^n = b^n + nb^{n-1} + \frac{n(n-1)}{2}b^{n-2} + \cdots \ge b^n + n + 1$, so that $a_n - b^n \ge n + 1 \ge 3$ contradicting (3).

6. Write a program to evaluate the expression $a^m \pmod m$ when $a = 2$ or 3 and m is
(i) 24479520371121008474792131183260228434377050031262 87, or
(ii) 59545797598759584957498579859585984759457948579595794859456799501.

Solutions (i) 818425157606843117638520752134598827774071621193626,
172619298139050924695876127082230361922144606801523 8.
(ii) 2, 3.

Pari script to solve 6.

```
;Compute $a^v(mod n)$
modexp(a,v,n)=
{
local(c,b);
c=a;
b=1;
while(v,
  if(v%2,
    b=b*c%n;
  ,);
  v=floor(v/2);
  c=c*c%n;
  );
return(b);
}

yy=244795203711210084747921311832602284343770500312628 7;
pp=595457975987595849574985798595859847594579485795957948594567995 01;
```