Math 467 Factorization and Primality Testing Fall Term 2024, Solutions 3

1. Write a program to find x and y such that $mx + ny = \gcd(m; n)$ where (i) $m = 8148657527$, $n = 8148653735$, (ii) $m = 8418785375$, $n = 7849911069$, (iii) $m = 4029583209458450398503$, $n = 3449459408504500003009$, (iv) $m = 304250263527210$, $n = 230958203482321$.

```
gcdx(a,b)=
{
local(r,rr,u,v,uu,vv);
r=a;
rr=b;
u=1;
v=0;
uu=0;
vv=1;
while(rr,
  qqq=floor(r/rr);
  rrr=r-qqq*rr;
  uuu=u-qqq*uu;
  vvv=v-qqq*vv;
  u=uu;
  v=vv;
  uu=uuu;
  vv=vvv;
  r=rr;
  rr=rrr;
  );
print("gcd(",a,",",b,") = ",r," = ",u,".",a," + ",v,".",b);
r=0;
if(r,break);
}
aa=8148657527;
bb=8148653735;
cc=8418785375;
dd=7849911069;
ee=4029583209458450398503;
ff=3449459408504500003009;
gg=304250263527210;
```

```
hh=230958203482321;
```

$$\gcd(8148657527, 8148653735) = 1 = (-1802932617)8148657527 + 1802933456 \times 8148653735$$
$$\gcd(8418785375, 7849911069) = 1001 = 2823598 \times 8418785375 + (-3028221)7849911069$$
$$\gcd(40295832094584503985 03, 34494594085045000030 09) = 1 =$$
$$230412343872401941219 \times 402958320945845039850 3 + (-269162672223683393684)344945940850450000300 9$$
$$\gcd(304250263527210, 230958203482321) = 203$$
$$= (-208202073629)304250263527210 + 274272724733 \times 230958203482321$$

2. Show that if $\gcd(a, b) = 1$, then $\gcd(a-b, a+b) = 1$ or 2. Exactly when is the value 2?

Let $d = \gcd(a-b, a+b)$. Then $d|a-b$ and $d|a+b$. Hence $d|(a+b)+(a-b) = 2a$ and $d|(a=b)-(a-b) = 2b$. Thus $d|\gcd(2a, 2b) = 2\gcd(a, b) = 2$. The case $d = 2$ occurs if and only if $2|a+b$ and $2|a-b$, i.e. a and b are of the same parity, but since $\gcd(a, b) = 1$ they both have to be odd.

3. The Fibonacci sequence (1202) is defined iteratively by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$. Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.

Proof by induction on n. Base case $n = 1$. Since $m|F_1 = 1$ we have $m = 1$. Now suppose result holds for every m with $m|F_{n-1}$ and $m|F_n$. Thus, when $m|F_{n+1}$ and $m|F_n$ we have $m|(F_{n+1} - F_n) = F_{n-1}$, so by the inductive hypothesis $m = 1$.

4. The squarefree numbers are the natural numbers which have no repeated prime factors, e.g 6, 105. Note that 1 is the only natural number which is both squarefree and a perfect square. Prove that every $n \in \mathbb{N}$ with $n > 1$ can be written uniquely as the product of a perfect square and a squarefree number.

By uniqueness of factorization $n = p_1^{k_1} \ldots p_s^{k_s}$ where the primes p_j are distinct and the exponents k_j are positive. Write $k_j = 2l_j + m_j$ where m_j is 0 when k_j is even and 1 when k_j is odd, and l_j is non-negative. Let $x = p_1^{l_1} \ldots p_s^{l_s}$ and $y = p_1^{m_1} \ldots p_s * m_s$. Then $n = x^2 y$ and y is squarefree.

5. Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Prove that the equations $\gcd(x, y) = a$ and $xy = b$ can be solved simultaneously in integers x and y if and only if $a^2|b$.

First suppose there are such x and y. Since $\gcd(x, y) = a$ we have $a|x$ and $a|y$, so that $a^2|xy = b$. Conversely suppose that $a^2|b$. Let $x = a$ and $y = b/a$. Then $xy = b$ and $a^2|b = ay$ so that $a|y$. Hence $\gcd(x, y) = a\gcd(1, y/a) = a$.