Homework 3

Suyi Liu

March 3, 2017

1 Problem 1

See extendedeuclid.m file with comments included

2 Problem 2

See inverse.m file with comments included
We are expecting input a and n relatively prime, since if they are not relatively prime, out subroutine extendedeuclid.m cannot find an ax + (-q)n = 1, thus no inverse exists.

3 Problem 3

- (a)
  by calling extendedeuclid function written in Problem 1, I get gcd(30030, 257) = 1

- (b)
  Suppose 257 is not prime, then there exists an integer x, $1 < x < 257$ such that x|257. **Then there must exists a prime integer $1 < y < 257$ such that y|257.** Because if x is a prime, we can let y=x, if x is not a prime, we can factorize it, and choose a prime number such that y|x, since y|x, x|257, then y|257.

  We can check all the prime integers from 1 to $\sqrt{257}$ to see if such y exists. We don't need to check prime integers beyond $\sqrt{257}$, since if there is a prime integer y"> $\sqrt{257}$ that y"|257, then y'y" = 257 and y' must < $\sqrt{257}$, so we have already find such y' in this case, and we can also factor y' to be a prime integer y that y|y' and thus y|257 because y'|257.

  So we check if any of 2,3,5,7,11,13 divide 257, because $\sqrt{257} > 16$ and

2,3,5,7,11,13 are all prime numbers < 16. From part (a), we know none of these prime numbers can divide 257 (because gcd(30030,257) = 1, if any of these numbers divides 257, then gcd(30030,257)$\neq$1, because each of these numbers divides 30030. Therefore causes contradiction.)

Since such y cannot be found, there doesn't exist any prime integer > 1 and < 257 that divides 257, so it contradicts our assumption that 257 is not prime. So 257 is prime.

4 Problem 4

- (a)
  by calling extendedeuclid function written in Problem 1, I get gcd(4883, 4369) = 257
- (b)
  $4883 = 19^1 * 257^1$ (since 19 and 257 are prime numbers)
  $4369 = 17^1 * 257^1$ (since 17 and 257 are prime numbers)

5 Problem 5

- (a)
  gcd(Fn, Fn1) = gcd(Fn-1, Fn-2) = gcd(Fn-2, Fn-3) = ... = gcd(1, 1) = 1
  Because Fi = Fi-1 + Fi-2, and because Fi-2 < Fi-1, Fi = 1 * Fi-1 + Fi-2, and $0 \leq$ Fi-2 < Fi-1
- (b)
  by calling extendedeuclid function written in Problem 1, I get gcd(11111111, 11111) = 1
- (c)
  gcd(a,b) = 1
  Because: gcd(11...11(n 1s), 11...1(n-1 1s)) = gcd(11...11(n-1 1s), 11...1(n-2 1s)) = ... = gcd(11,1) = 1
  This is because 11...11(n 1s) = 10 * 11...1(n-1 1s) + 1, $0 \leq 1 <$ 11...1(n-1 1s).

6 Problem 6

- (a)
  For all of x, the absolute value of p(x) is prime.

```
for i=0:61
    p=8*i*i-488*i+7243
```

```
    if p>0
        isprime(p)
    else
        isprime(-p)
    end
end
```

- (b)
  For all of x, the absolute value of p(x) is prime.

  ```
  for i=0:19
      p=i*i*i*i+29*i*i+101
      if p>0
          isprime(p)
      else
          isprime(-p)
      end
  end
  ```

- (c)
  Suppose there exists nonconstant polynomial $q(x) = a_1x^n + a_2x^{n-1} + ... + a_nx + c$, and $q(x)$ is prime for all positive integers x

  Suppose g is a positive integer, $q(g) = a_1g^n + a_2g^{n-1} + ... + a_ng + c = b$, and b is also a positive integer(if not, try another g until we get a positive integer), and by assumption, b is prime.

  then $q(g+b) = a_1(g+b)^n + a_2(g+b)^{n-1} + ... + a_n(g+b) + c = a_1(g^n + \alpha + \beta + ... + b^n) + a_2(g^{n-1} + \alpha' + \beta' + ... + b^{n-1}) + ... + c = (a_1g^n + a_2g^{n-1} + ... + a_ng + c) + \gamma = q(g) + \gamma$. Where α, β, ... α', β' all are multiples of b(suggested by binomial theorem), and γ is the sum of them, so in this case γ is also a multiple of b

  Since $q(g) = b$ and $b|\gamma$, $b|b+\gamma$, $b|q(g+b)$.
  Since by assumption, $q(g+b)$ is also a prime, it must be that $b = q(g+b)$ (Because b and $q(g+b)$ are primes, so they are both not 1, and if $b \neq q(g+b)$, then $q(g+b)$ will not be a prime, contradiction), that is $q(g) = q(g+b)$, so we can use the same logic to infer $q(g) = q(g+b) = q(g+b+b) = ... = q(g+kb)$

  Since $q(x)$ remains same for infinite number of points $x = g = kb$, it is actually a constant polynomial, thus leads to a contradiction.
  So there does not exist a nonconstant polynomial $q(x)$ with integer coefficients such that for all positive integers x it holds that $q(x)$ is prime.