Computational Number Theory - Homework 1

Philip Warton

January 15, 2021

Problem 1

(a)

$$64 = (5)11 + 9$$

(b)

$$-50 = (-8)7 + 6$$

(c)

$$91 = (7)13 + 0$$

(d)

$$11 = (0)15 + 11$$

Problem 2

Prove that $6|n^3 - n$ for all $n \in \mathbb{N}$.

Proof.

$$\begin{aligned}
0^3 - 0 &= 0 \\
1^3 - 1 &= 1 \\
2^3 - 2 &= 6 \\
3^3 - 3 &= 24 \\
4^3 - 4 &= 60 \\
5^3 - 5 &= 120
\end{aligned}$$

Now let $n > 5$. We write $n = q6 + r$. Then we write

$$\begin{aligned}
n^3 - n &= (q6 + r)^3 - (q6 + r) \\
&= (6^2q^2 + 6(2)rq + r^2)(6q + r) - (q6 + r) \\
&= (6^3q^3 + 6^2(2)rq^2 + 6r^2q + 6^2q^2r + 6(2)r^2q + r^3) - (6q + r) \\
&= (6)(6^2q^3 + 6(2)rq^2 + r^2q + 6q^2r + (2)r^2q - q) + (r^3 - r)
\end{aligned}$$

Then the first term is clearly divisible by 6, and since $r \in \{0, 1, 2, 3, 4, 5\}$ we know that the second term is also divisible by 6. $\square$

Problem 3

(a)

Let p be a prime number which is not 2 or 3. Show that when p is divided by 6, the remainder is either 1 or 5.

Proof. Suppose that the remainder is 2, then it follows that $2|p$ since the number is even. Suppose that the remainder is 3 then it follows that $3|p$. If the remainder is 4, then $2|p$ since p must be even. $\square$

(b)

Show that the product of two numbers of the form $6x + 1$ is also of the form $6x + 1$.

Proof. Let $x, y \in \mathbb{Z}$. We say that $(6x + 1)(6y + 1) = 6^2xy + 6y + 6x + 1 = 6(6xy + y + x) + 1$, which is of the described form $6k + 1$. □

(c)

Show that if k is a positive integer, then $6k + 5$ has a prime factor p of the form $p = 6x + 5$.

Proof. Let $k \in \mathbb{Z}^+$. We want to show that $6k + 5$ has a prime factor p of the form $p = 6x + 5$. Suppose that each prime factor is not of the form $6x + 5$. Then they must all be of the form $6x + 1$, since any prime number that is not 2 or 3 has remainder of either 1 or 5. But in this case, their product would be of the form $6x + 1$. Therefore it must be the case that there is some prime factor of $6k + 5$ that is of that same form. □

(d)

Suppose there is a finite number of primes of the form $6x + 5$. Construct a set containing each of these denoted by $\{q_1, q_2, q_3, \cdots q_k\}$. Then let $Q = \Pi_{i=1}^{k} q_i$. If k is even, $Q \equiv [1]_6$, otherwise $Q \equiv [5]_6$.

$\boxed{\text{Case 1: } k \text{ is even}}$ Let $p = Q + 4 \equiv [5]_6$. In other words, $\exists k \in \mathbb{N}$ such that $p = 6k + 5$. Therefore it must have a prime factor of the form $p' = 6x + 5$. It must be equal to some q_i, since it is a prime of the form $6x + 5$. Therefore it must divide Q. Thus $p'|Q$ and $p'|Q + 4$. However, it cannot be the case that p' divides 4, since 4's only prime factor 2 is not of the form $6x + 5$. This means that $p'|p - Q = 4$ but $p' \nmid 4$ (contradiction).

$\boxed{\text{Case 2: } k \text{ is odd}}$ Let $p = Q + 6 \equiv [5]_6$. Then it must be of the form $6k + 5$ for some $k \in \mathbb{N}$. Therefore it must have some prime factor p' of the form $6x + 5$. Then it must be the case that $p'|Q$ and that $p'|p$. However this means $p'|p - Q = 6$, but 6 is not of the form $6x + 5$ (contradiction).

Problem 4

(a)

Proof. Suppose that $\gcd(a, b) = 1$, and $a|c$ and $b|c$. Then $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. We want to show that there exists k such that $c = k(ab)$. There exists $k_a, k_b \in \mathbb{Z}$ such that $c = k_a(a), c = k_b(b)$. So we can write the following:

$$\begin{aligned} c &= c(1) \\ &= c(ax + by) \\ &= cax + cby \\ &= k_b(b)(ax) + k_a(a)(by) \\ &= ab(k_bx) + ab(k_ay) \\ &= ab(k_bx + k_ay) \end{aligned}$$

□

(b)

Proof. Suppose that $\gcd(a, b) = 1$ and that $a|bc$. Then write $bc = k_a(a)$ and $ax + by = 1$. We have the following:

$$\begin{aligned} c &= c(1) \\ &= c(ax + by) \\ &= cax + cby \\ &= cax + (bc)y \\ &= cax + k_a(a)y \\ &= a(cx + k_ay) \end{aligned}$$

□

(c)

Proof. Suppose that p is prime and that $p|ab$. If $\gcd(p,a)=1$, then $p|b$. Otherwise, it must be the case that $\gcd(p,a)=p$ (since p has no factors other than 1 and p) and therefore $p|a$. □

(d)

Proof. Let $x \in \mathbb{Z}$. Suppose $\gcd(6x+5, 5x+4) \neq 1$. Then there must be some number not equal to 1 that divides both. □

Problem 5

Use the extended Euclidean algorithm to solve $ax+by=\gcd(a,b)$.

(a)

Let $a=-23, b=16$.

$$\begin{aligned} -23 &= -2(16)+9 \\ 16 &= 1(9)+7 \\ 9 &= 1(7)+2 \\ 7 &= 3(2)+1 \end{aligned}$$

$$\begin{aligned} 7-3(2) &= 1 \\ 4(7)-3(9) &= 1 \\ 4(16)-7(9) &= 1 \\ -10(16)-7(-23) &= 1 \end{aligned}$$

(b)

Let $a=111, b=442$.

$$\begin{aligned} 442 &= 3(111)+109 \\ 111 &= 1(109)+2 \\ 109 &= 54(2)+1 \end{aligned}$$

$$\begin{aligned} 109-54(2) &= 1 \\ 109-54(111-109) &= 1 \\ 55(109)-54(111) &= 1 \\ 55(442-3(111))-54(111) &= 1 \\ 55(442)-219(111) &= 1 \end{aligned}$$

Problem 6

(i)

To count the number of primes we run the following:

Code:

```
count = 0
for n in range(100,999):
    if is_prime(n):
        count = count + 1
print(count)
```

Output:

```
    143
```

There are a total of 143 prime numbers that have 3 digits.

(ii)

To find the smallest 3 primes with 10 digits we run the following:

Code:

```
count = 0
num = 1000000000
while count < 3:
    if is_prime(num):
        print(num)
        count = count + 1
    num = num + 1
```

Output:

```
1000000007
1000000009
1000000021
```

(iii)

To list and count all primes of the form $10^3 \leqslant n^2 + 1 < 10^4$ we run the following Sage code:

Code:

```
start = floor(sqrt(1000)) - 1
end = ceil(sqrt(10000)) + 1
count = 0
for number in range(start, end):
    x = number^2 + 1
    if is_prime(x):
        print(x)
    count = count + 1
print("\nCOUNT: ", count)
```

Output:

```
1297
1601
2917
3137
4357
5477
7057
8101
8837

COUNT:  9
```