Math 3200

Homework 3

(2.2) Compute the following gcd's using Algorithm 1.1.13.

$$\gcd(15, 35) \qquad \gcd(247, 299) \qquad \gcd(51, 897) \qquad \gcd(136, 304)$$

Show all of your work. Feel free to use python to do (and display) the computations, but in this case also turn in a printout of your code.

---

solution: I used a python program to do this problem. First the code.

```
# Algorithm 1.1.13
def gcd(a,b):
    a,b = abs(a),abs(b)
    while b != 0:

        # a = q(b)+(r)
        q,r = divmod(a,b)

        print('{} = {}({})+({})'.format(a,q,b,r))

        a,b = b,r

    return a
```

Next the results from running `gcd` on the four cases.

```
In [2]: gcd(15,35)
15 = 0(35)+(15)
35 = 2(15)+(5)
15 = 3(5)+(0)
Out[2]: 5
```

```
In [3]: gcd(247,299)
247 = 0(299)+(247)
299 = 1(247)+(52)
247 = 4(52)+(39)
52 = 1(39)+(13)
39 = 3(13)+(0)
Out[3]: 13
```

```
In [4]: gcd(51,897)
51 = 0(897)+(51)
897 = 17(51)+(30)
51 = 1(30)+(21)
30 = 1(21)+(9)
21 = 2(9)+(3)
9 = 3(3)+(0)
Out[4]: 3
```

```
In [5]: gcd(136,304)
136 = 0(304)+(136)
304 = 2(136)+(32)
136 = 4(32)+(8)
32 = 4(8)+(0)
Out[5]: 8
```

(2.7) Find four complete sets of residues modulo 7, where the ith set satisfies the ith condition: (1) nonnegative, (2) odd, (3) even, (4) prime.

---

solution: There are an infinite number of solutions for each condition. Here's a selection:

(1) nonnegative	$\{0, 1, 2, 3, 4, 5, 6\}$
(2) odd	$\{7, 1, 9, 3, 11, 5, 13\}$
(3) even	$\{0, 8, 2, 10, 4, 12, 6\}$
(4) prime	$\{7, 29, 2, 3, 11, 5, 13\}$

(2.8) Find rules in the spirit of Proposition 2.1.9 for divisibility of an integer by 5, 9, and 11, and prove each of these rules using arithmetic modulo a suitable n.

---

solution: For all of these we will consider $10^k \pmod{n}$ for $k = 0, 1, 2, \ldots$. This will allow us to easily reduce any integer m modulo n by considering its decimal representation $m = \sum_{k\geq 0} d_k 10^k$.

(5) Since $10 \equiv 0 \pmod{5}$, we have $10^k \equiv 0 \pmod{5}$ for all $k > 0$ so $m \equiv d_0 \pmod{5}$ and m is divisible by 5 if and only if the "ones" digit d_0 is so divisible: $d_0 = 5$ or 10.

(9) Since $10 \equiv 1 \pmod{9}$, we have $10^k \equiv 1 \pmod{9}$ for all $k \geq 0$ so $m \equiv \sum_{k\geq 0} d_k \pmod{9}$ and m is divisible by 9 if and only if the sum of the digits $\sum_{k\geq 0} d_k$ is so divisible.

(11) Since $10 \equiv -1 \pmod{11}$, we have $10^k \equiv -1 \pmod{11}$ for odd $k \geq 0$ and $10^k \equiv 1 \pmod{11}$ for even $k \geq 0$. Consequently $m \equiv \sum_{k\geq 0}(-1)^k d_k \pmod{11}$ and m is divisible by 11 if and only if the alternating sum of the digits $\sum_{k\geq 0}(-1)^k d_k$ is so divisible.

(2.24) Prove that for any postive integer n the fraction $(12n + 1)/(30n + 2)$ is in reduced form.

---

solution: All that has to be shown is that for any positive integer n $\gcd(12n + 1, 30n + 2) = 1$. We'll do this in an ad hoc fashion.

$$\begin{aligned}\gcd(12n + 1, 30n + 2) &= \gcd(12n + 1, 15n + 1)\\ &= \gcd(12n + 1, 3n)\\ &= \gcd(1, 3n)\\ &= 1\end{aligned}$$

(2.9) (Optional Challenge problem) *(The following problem is from the 1998 Putnam Competition.)* Define a sequence of decimal integers a_n as follows: $a_1 = 0$, $a_2 = 1$, and a_{n+2} is obtained by writing the digits of a_{n+1} immediately followed by those of a_n. For example $a_3 = 10$, $a_4 = 101$, and $a_5 = 10110$. Determine the n such that a_n is a multiple of 11, as follows:

(a) Find the smallest integer $n > 1$ such that a_n is divisible by 11.

(b) Prove that a_n is divisible by 11 if and only if $n \equiv 1 \pmod 6$.

---

solution: Let d_{nk} be the k^{th} digit of a_n. Let b_n be the parity of the bit length of a_n and let c_n be the alternating sum $\sum_k (-1)^k d_{nk}$. We'll use the characterization of divisibility by 11 from Exercise 2.8, namely a_n is divisible by 11 if and only if c_n is so divisible.

The term a_{n+2} is constructed from a_n and a version of a_{n+1} that has been shifted by b_n, the bit length of a_n. After some reflection we see that we have have the following two recursive relations:

$$b_{n+2} = b_{n+1} + b_n \pmod 2$$
$$c_{n+2} = (-1)^{b_n} c_{n+1} + c_n \pmod{11}$$

that hold for $n \geq 1$. Coupling this with the given information: $a_1 = 0$ and $a_2 = 1$ we can construct the table:

n	a_n	b_n	c_n
1	0	1	0
2	1	1	1
3	10	0	-1
4	101	1	2
5	10110	1	1
6	10110101	0	1
7	1011010110110	1	0
8	101101011011010110101	1	1

Since the next row is determined by the previous two and the b_n and c_n columns in rows 7 and 8 are the same as those columns in rows 1 and 2, from this point on these columns will repeat themselves and we have:

$$c_n = \begin{cases} 0 & n \equiv 1 \pmod 6 \\ 1 & n \equiv 2 \pmod 6 \\ -1 & n \equiv 3 \pmod 6 \\ 2 & n \equiv 4 \pmod 6 \\ 1 & n \equiv 5 \pmod 6 \\ 1 & n \equiv 0 \pmod 6 \end{cases}$$

We see that c_n (and so a_n) is divisible by 11 iff $n \equiv 1 \pmod 6$ and the smallest such $n > 1$ is 7.