Lectures 15 and 16

We introduced the Euclidean Algorithm to find the $\gcd(n, m)$.

We showed that the $\gcd(n, m)$ can be found in at most $2\log_2(n)$ steps if $n > n$.

We showed how the algorithm can be extended to find λ and μ so that

$$\lambda n + \mu m = \gcd(n, m)$$

First application of the Euclidean Algorithm was to complete the proof that

$$[(p \mid ab) \Rightarrow (p \mid a) \vee (p \mid b)] \iff [(p = ab) \Rightarrow (a = \pm 1) \vee (b = \pm 1)]$$

and then to show that each $n \in \mathbb{Z}$ is *uniquely* factorable into primes.

Lastly we introduced modular arithmetic, e.g. $8 + 7 \equiv 4 \bmod 11$ and $8 \cdot 7 \equiv 10 \bmod 11$, a commutative, associative and distributive addition and multiplication on the remainder set modulo n, $\mathbb{Z}_n$.

Exercises for Lectures 15 and 16

1. Find the greatest common divisor of 321 and 123. Find λ and μ so that

$$\lambda 321 + \mu 123 = \gcd(321, 123)$$

2. Find the greatest common divisor of 111 and 111. Find λ and μ so that

$$\lambda 111 + \mu 1111 = \gcd(111, 1111)$$

3. Find the greatest common divisor of 2016 and 1997. Find λ and μ so that

$$\lambda 2016 + \mu 1997 = \gcd(2016, 1997)$$

4. Find the greatest common divisor of 2016 and 1997. Find λ and μ so that

$$\lambda 2016 + \mu 1997 = \gcd(2016, 1997)$$

5. Find two 2-digit numbers (base 10) for which the Euclidean algorithm requires 7 steps to find the gcd.

6. Fill in the addition and multiplication tables for arithmetic modulo 5.

+	0	1	2	3	4
0					
1					
2					
3					
4					

×	0	1	2	3	4
0					
1					
2					
3					
4					

7. Make addition and multiplication tables for arithmetic modulo 12.
8. Make addition and multiplication tables for arithmetic modulo 13.
9. Let p, q and r be three distinct primes. Show that $spq^2 + tqp^2 = r$ has no solutions s and t in the integers.