

# Schedule

A week-by-week breakdown of the material.

## Week 1 (01/05-01/09)

- Day 1
  - Numbers: Rationals, Reals, Complex<sup>1</sup>
  - Basic proof techniques: Direct<sup>2</sup>
  - Assignment 1<sup>3</sup>
- Day 2
  - Basic proof techniques: Indirect<sup>4</sup>
  - Square root of 2 is irrational<sup>5</sup>
- Day 3
  - Quantifiers<sup>6</sup>
  - Principle of Mathematical Induction<sup>7</sup>
  - Assignment 2<sup>8</sup>
- Day 4
  - Strong induction and Well-Ordering Principle<sup>9</sup>
  - Fibonacci Numbers<sup>10</sup>

## Week 2 (01/12-01/16)

- Day 1
  - Divisibility<sup>11</sup>
- Day 2
  - Prime and Composite Numbers<sup>12</sup>

---

<sup>1</sup>[notes/numbers\\_intro.html](#)

<sup>2</sup>[notes/proofs\\_basic.html](#)

<sup>3</sup>[assignments/1.html](#)

<sup>4</sup>[notes/proofs\\_basic.html](#)

<sup>5</sup>[notes/irrationality\\_of\\_sqrt2.html](#)

<sup>6</sup>[notes/proofs\\_quantifiers.html](#)

<sup>7</sup>[notes/proofs\\_induction.html](#)

<sup>8</sup>[assignments/2.html](#)

<sup>9</sup>[notes/proofs\\_induction\\_other.html](#)

<sup>10</sup>[notes/numbers\\_fibonacci.html](#)

<sup>11</sup>[notes/numbers\\_divisibility.html](#)

<sup>12</sup>[notes/primes\\_intro.html](#)

- Assignment 3<sup>13</sup>
- Day 3
  - Patterns in the Primes<sup>14</sup>
  - Common Divisors<sup>15</sup>
- Day 4
  - The Division Theorem<sup>16</sup>

## Week 3 (01/19-01/23)

- Day 1
  - A weird number system<sup>17</sup>
  - The Division Theorem (cont)<sup>18</sup>
  - Assignment 4<sup>19</sup>
- Day 2
  - The Euclidean Algorithm<sup>20</sup>
- Day 3
  - Diophantine Equations<sup>21</sup>
  - Euclidean Division and Diophantine Equations<sup>22</sup>
- Day 4
  - Finding all Solutions<sup>23</sup>
  - Assignment 5<sup>24</sup>

## Week 4 (01/26-01/30)

- Day 1
  - Finding all Solutions (cont)<sup>25</sup>

---

<sup>13</sup>[assignments/3.html](#)

<sup>14</sup>[notes/primes\\_patterns.html](#)

<sup>15</sup>[notes/numbers\\_gcd.html](#)

<sup>16</sup>[notes/numbers\\_division\\_theorem.html](#)

<sup>17</sup>[notes/weird\\_number\\_system.html](#)

<sup>18</sup>[notes/numbers\\_division\\_theorem.html](#)

<sup>19</sup>[assignments/4.html](#)

<sup>20</sup>[notes/numbers\\_euclidean\\_algorithm.html](#)

<sup>21</sup>[notes/equations\\_diophantine\\_intro.html](#)

<sup>22</sup>[notes/equations\\_diophantine\\_and\\_euclidean.html](#)

<sup>23</sup>[notes/equations\\_diophantine\\_all\\_solutions.html](#)

<sup>24</sup>[assignments/5.html](#)

<sup>25</sup>[notes/equations\\_diophantine\\_all\\_solutions.html](#)

- Fundamental Theorem of Arithmetic<sup>26</sup>
- Day 2
  - Consequences of Fundamental Theorem<sup>27</sup>
- Day 3
  - Modular Arithmetic and Congruences<sup>28</sup>
- Day 4
  - Arithmetic with Congruences<sup>29</sup>

## Week 5 (02/02-02/06)

- Day 1
  - Review
- Day 2
  - MIDTERM
- Day 3
  - Chinese Remainder Theorem<sup>30</sup>
  - Assignment 6<sup>31</sup>
- Day 4
  - Congruence Classes as a Number System<sup>32</sup>

## Week 6 (02/09-02/13)

- Day 1
  - Multiplicative Inverses<sup>33</sup>
- Day 2
  - Multiplicative Inverses (cont)<sup>34</sup>
- Day 3

---

<sup>26</sup>[notes/numbers\\_fundamental\\_theorem.html](#)

<sup>27</sup>[notes/numbers\\_fta\\_consequences.html](#)

<sup>28</sup>[notes/congruence\\_intro.html](#)

<sup>29</sup>[notes/congruence\\_arithmetic.html](#)

<sup>30</sup>[notes/congruence\\_chinese\\_remainder.html](#)

<sup>31</sup>[assignments/6.html](#)

<sup>32</sup>[notes/congruence\\_system.html](#)

<sup>33</sup>[notes/congruence\\_multiplicative\\_inverses.html](#)

<sup>34</sup>[notes/congruence\\_multiplicative\\_inverses.html](#)

- Basics of Encryption<sup>35</sup>
- Encryption via Multiplication<sup>36</sup>
- Day 4
  - Fermat's Little Theorem<sup>37</sup>
  - Assignment 7<sup>38</sup>

## Week 7 (02/16-02/20)

- Day 1
- Day 2
  - Reduced Residues and  $\phi$ <sup>39</sup>
- Day 3
  - Reduced Residues and  $\phi$  (cont)<sup>40</sup>
- Day 4
  - Euler's Theorem<sup>41</sup>

## Week 8 (02/23-02/27)

BREAK

## Week 9 (03/02-03/06)

- Day 1
- Day 2
- Day 3
  - Fast exponentiation<sup>42</sup>
- Day 4
  - Encryption via Exponentiation<sup>43</sup>

---

<sup>35</sup>[notes/encryption\\_basic.html](#)

<sup>36</sup>[notes/encryption\\_mult.html](#)

<sup>37</sup>[notes/congruence\\_fermats.html](#)

<sup>38</sup>[assignments/7.html](#)

<sup>39</sup>[notes/residues\\_basic.html](#)

<sup>40</sup>[notes/residues\\_basic.html](#)

<sup>41</sup>[notes/residues\\_eulers\\_theorem.html](#)

<sup>42</sup>[notes/residues\\_exponentiation.html](#)

<sup>43</sup>[notes/encryption\\_exp.html](#)

## Week 10 (03/09-03/13)

- Day 1
  - Public Keys and RSA<sup>44</sup>
- Day 2
  - Order of Elements in  $\mathbb{Z}_n$ <sup>45</sup>
- Day 3
  - Polynomials over  $\mathbb{Z}_n$ <sup>46</sup>
- Day 4
  - Primitive Roots<sup>47</sup>

## Week 11 (03/16-03/20)

- Day 1
  - Primitive Root Theorem<sup>48</sup>
- Day 2
  - MIDTERM
  - Applications of Primitive Roots: Diffie-Hellman protocol<sup>49</sup>
- Day 3
  - Congruential Random Number Generators<sup>50</sup>
- Day 4

## Week 12 (03/23-03/27)

- Day 1
  - Quadratic Residues<sup>51</sup>
- Day 2
  - The Legendre Symbol<sup>52</sup>

---

<sup>44</sup>[notes/encryption\\_rsa.html](#)

<sup>45</sup>[notes/residues\\_order.html](#)

<sup>46</sup>[notes/residues\\_polynomials.html](#)

<sup>47</sup>[notes/residues\\_primitive\\_roots.html](#)

<sup>48</sup>[notes/residues\\_primitive\\_root\\_theorem.html](#)

<sup>49</sup>[notes/encryption\\_diffie\\_hellman.html](#)

<sup>50</sup>[notes/numbers\\_random.html](#)

<sup>51</sup>[notes/residues\\_quadratic.html](#)

<sup>52</sup>[notes/residues\\_legendre.html](#)

- Day 3
  - Euler's Identity<sup>53</sup>
- Day 4
  - Properties of Legendre symbol<sup>54</sup>

### **Week 13 (03/30-04/03)**

- Day 1
  - Law of Quadratic Reciprocity<sup>55</sup>
- Day 2
  - Gauss's Lemma<sup>56</sup>
- Day 3
- Day 4

### **Week 14 (04/06-04/10)**

- Day 1
- Day 2
- Day 3
- Day 4

---

<sup>53</sup>[notes/residues\\_eulers\\_identity.html](#)

<sup>54</sup>[notes/residues\\_legendre\\_properties.html](#)

<sup>55</sup>[notes/residues\\_reciprocity.html](#)

<sup>56</sup>[notes/residues\\_gauss\\_lemma.html](#)