Introduction to Number Theory

• Topics we will cover
  – Prime numbers
  – Fermat’s and Euler’s Theorem
  – Testing for Primality
    • Algorithms will be probabilistic with a high degree of certainty
    • Algorithms use Fermat’s and Euler’s Theorem
  – The Chinese Remainder Theorem
    • Used to solve problems in smaller domains
    • Pollard’s Rho uses CRT to factor the product of large primes
      (materials from an alternate textbook)
  – Discrete Logarithms, the basis of Elliptic Curve Encryption
Why We Need Number Theory

• Overview of asymmetric encryption
  – How does public key encryption work?
  – How are modular exponential values calculated?
  – How hard is it to find prime numbers?
  – How hard is it to factor the product of two large primes?

• The RSA scheme was devised in 1978
  – RSA stands for Rivest, Shamir, Aldeman
  – The public key approach does not require mutual knowledge of a secret key, thus it is appropriate for secure information transfer over the Internet
  – However the transfer of large amounts of information is best done using a secret key; the RSA scheme can be used to share this key
Prime Numbers

• Who can formally define a prime number?
• Starting at 2 (the only even prime number), list the first few prime numbers sequentially
• Does anyone know the fundamental theorem of arithmetic?
• The RSA scheme depends on
  – It is easy to find large prime numbers
  – It is difficult to factor the product of two large primes
• We need to work with modular arithmetic; why does this make sense in computer science?
### Primes Less Than 2000

|    | 2   | 3   | 5   | 7   | 11  | 13  | 17  | 19  | 23  | 29  | 31  | 37  | 41  | 43  | 47  | 53  | 59  | 61  | 67  | 71  | 73  | 79  | 83  | 89  | 97  |
|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 101| 103 | 107 | 109 | 113 | 127 | 131 | 137 | 139 | 149 | 151 | 157 | 163 | 167 | 173 | 179 | 181 | 191 | 193 | 197 | 199 |
| 211| 223 | 227 | 229 | 233 | 239 | 241 | 251 | 257 | 263 | 269 | 271 | 277 | 281 | 283 | 293 |
| 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 | 353 | 359 | 367 | 373 | 379 | 383 | 389 | 397 |
| 401 | 409 | 421 | 431 | 433 | 439 | 443 | 449 | 457 | 461 | 463 | 467 | 479 | 487 | 491 | 499 |
| 503 | 509 | 521 | 523 | 541 | 547 | 557 | 563 | 569 | 571 | 577 | 587 | 593 | 599 |
| 601 | 607 | 613 | 617 | 619 | 631 | 641 | 643 | 647 | 653 | 659 | 661 | 673 | 677 | 683 | 691 |
| 701 | 709 | 719 | 727 | 733 | 739 | 743 | 751 | 757 | 761 | 769 | 773 | 787 | 797 |
| 809 | 811 | 821 | 823 | 827 | 829 | 839 | 853 | 857 | 859 | 863 | 877 | 881 | 883 | 887 |
| 907 | 911 | 919 | 929 | 937 | 941 | 947 | 953 | 967 | 971 | 977 | 983 | 991 | 997 |
| 1009 | 1013 | 1019 | 1021 | 1031 | 1033 | 1039 | 1049 | 1051 | 1061 | 1063 | 1069 | 1087 | 1091 | 1093 | 1097 |
| 1103 | 1109 | 1117 | 1123 | 1129 | 1151 | 1153 | 1163 | 1171 | 1181 | 1187 | 1193 |
| 1201 | 1217 | 1223 | 1229 | 1231 | 1249 | 1259 | 1277 | 1279 | 1283 | 1289 | 1291 | 1297 |
| 1301 | 1307 | 1319 | 1321 | 1327 | 1361 | 1367 | 1373 | 1381 | 1399 |
| 1409 | 1423 | 1427 | 1429 | 1433 | 1439 | 1447 | 1451 | 1453 | 1459 | 1471 | 1481 | 1483 | 1487 | 1489 | 1493 | 1499 |
| 1511 | 1523 | 1531 | 1543 | 1549 | 1553 | 1559 | 1567 | 1571 | 1579 | 1583 | 1589 | 1597 |
| 1601 | 1607 | 1609 | 1613 | 1619 | 1621 | 1627 | 1637 | 1657 | 1663 | 1667 | 1669 | 1693 | 1699 |
| 1709 | 1721 | 1723 | 1733 | 1741 | 1747 | 1753 | 1759 | 1777 | 1783 | 1787 | 1789 |
| 1801 | 1811 | 1823 | 1831 | 1847 | 1861 | 1867 | 1871 | 1873 | 1877 | 1879 | 1889 |

- Make a conjecture about the density of primes
The Density of Primes

– primes are reasonably dense, so finding a large prime should not be too time consuming

– the prime distribution function $\pi(n)$ gives the number of primes $\leq n$

\[ \lim_{n \to \infty} \frac{\pi(n)}{n} = 1. \]

\textit{Theorem 33.37 (Prime number theorem)}

– For $n = 10^9$, $\pi(n) = 50,847,478$ and $n/\ln n = 48,254,942$ which is less than 6% error

– the probability a random integer $n$ is prime is $1/\ln n$

– for a hundred digit number, approximately 115 odd numbers would need to be tested to find a prime

– We will develop an algorithm to find large primes but we need to develop some math theory first
Fermat’s Theorem

• If p is prime and if a is a positive integer not divisible by p, then \( a^{p-1} \equiv 1 \mod p \)
  
  – the formal proof of this theorem given in the text is interesting reading
  
  – You will not be responsible for the proof on homework or exams but be aware that cryptography is based on mathematics

• What is the converse of the logical implication of \( p \Rightarrow q \)?

• What is the converse of Fermat’s Theorem?

• Is the converse of a theorem always true?
Euler’s Function

• Some background
  – What does it mean for two numbers to be relatively prime?
  – \( \phi(n) \) is the number of positive integers less than \( n \) that are relatively prime to \( n \)

• Some examples
  – Find \( \phi(19) \)
  – Find \( \phi(18) \)

• If \( n = p \times q \) where \( p \) and \( q \) are prime, then
  \[ \phi(n) = (p-1) \times (q-1) \]
  Why is this true?
Euler’s Theorem

- For every $a$ and $n$ that are relatively prime, $a^{\phi(n)} \equiv 1 \pmod{n}$

- Some examples
  - Suppose $a = 2$ and $n = 7$, then $\phi(7) = 6$, $2^6 = 64$ and $64 \pmod{7} = 1$
  - Suppose $a = 3$ and $n = 7$, then $\phi(7) = 6$, $3^6 = 729$ and $729 \pmod{7} = 1$

- An alternative form: $a^{\phi(n)+1} \equiv a \pmod{n}$

- A corollary: $m^{k\phi(n)+1} \equiv m \pmod{n}$

- If any number has a nontrivial root of 1, then the number must be composite
Group Work

- Some facts about $\phi(n)$: $\phi(p^i) = p^i - p^{i-1}$ if $p$ is prime and $\phi(mn) = \phi(n) * \phi(n)$ if $m,n$ are relatively prime
- Find $\phi(27)$

- Find $\phi(231)$
Miller-Rabin Primality Testing

- This is an alternative to the algorithm in the textbook; both are logically equivalent

\[
\text{WITNESS}(a, n)
\]

1. let \( n - 1 = 2^t u \), where \( t \geq 1 \) and \( u \) is odd
2. \( x_0 \leftarrow \text{MODULAR-EXponentiation}(a, u, n) \)
3. for \( i \leftarrow 1 \) to \( t \)
   
   \[
   \text{do } x_i \leftarrow x_{i-1}^2 \mod n
   \]
   
   if \( x_i = 1 \) and \( x_{i-1} \neq 1 \) and \( x_{i-1} \neq n - 1 \)
      
      then return \( \text{TRUE} \)
  
if \( x_t \neq 1 \)
   
   then return \( \text{TRUE} \)

9. return \( \text{FALSE} \)

Very likely the number is prime, but not for sure

Returns \( a^u \mod n \)

Nontrivial root of 1, so must be composite

Must be composite due to Fermat's theorem
Miller-Rabin Algorithm

**Miller-Rabin**\((n, s)\)

1. \textbf{for} \(j \leftarrow 1\) \textbf{to} \(s\)
2. \hspace{1em} \textbf{do} \(a \leftarrow \text{RANDOM}(1, n - 1)\)
3. \hspace{2em} \textbf{if} \ \text{WITNESS}(a, n)
4. \hspace{3em} \textbf{then} \textbf{return} \ \text{COMPOSITE} \hspace{1em} \triangleright \text{Definitely.}
5. \hspace{2em} \textbf{return} \ \text{PRIME} \hspace{1em} \triangleright \text{Almost surely.}

- \(s\) is the number of witnesses to be chosen randomly
- If any witness is found, \(n\) must be composite
- For a \(\beta\)-bit number, Miller-Rabin requires \(O(s \beta)\) arithmetic operations and \(O(s \beta^3)\) bit operations
Error rate for Miller-Rabin

• Error rate for witnesses
  – Returns “may be prime” for at most \((n-1)/4\) witness values
  – This means each test can be wrong at most \(\frac{1}{4}\) of the time; so repeated applications of witness will continually reduce the probability of an error

• Choice of \(s\)
  – if \(s\) is 25, then the probability of an error is “infinitesimally small” (less than \(4^{-25} = 2^{-50}\))
  – smaller values of \(s\) are good enough for most applications
Group Work

- If n is an odd composite integer, show that Miller-Rabin will return “may be prime” for $a = 1$ and $a = n-1$
The Chinese Remainder Theorem

• The assumptions
  – Let \( M = \prod_{i=1}^{k} m_i \) where the \( m_i \) are relatively prime
  – for our purposes the \( m_i \) can be the prime factorization of \( M \), thus they are all relatively prime
  – Any number \( A \) in \( Z_m \), can be represented by a \( k \)-tuple \((a_1, \ldots, a_k)\) where \( a_i \) is in \( Z_{m_i} \)

• The Conclusions
  – There is a 1-to-1 correspondence between \( Z_M \) and \( Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_k} \)
  – In particular, addition and multiplication in \( Z_M \) can be performed in the smaller domains
Conversion

• From A to \((a_1, a_2, \ldots, a_k)\)
  – Suppose \(M = 19 \times 37 = 703\), Let \(A = 500\)
  – Then \(500 \mod 19 = 6\) and \(500 \mod 37 = 19\), so 500 corresponds to the pair \((6, 19)\)

• From \((a_1, a_2, \ldots, a_k)\) to A
  – Where \(M_i = M/m_i\) define
    \[ c_i = M_i \times \left( M_i^{-1} \mod m_i \right) \text{ for } 0 \leq i \leq k \]
  – Then \(A \equiv \left( \sum_{i=1}^{k} a_i c_i \right) \mod M\)
  – \(M_1 = 37\) so \(M_1^{-1} = 18\) since \(37 \times 18 \equiv 1 \mod 19\)
  – \(M_2 = 19\) so \(M_2^{-1} = 2\) since \(19 \times 2 \equiv 1 \mod 37\)
  – So \(A = (6 \times 37 \times 18 + 19 \times 19 \times 2) \mod 703 = (3996 + 722) \mod 703 = 500\)
Operations – an example

• Operands
  – $87 \mod 703 = (87 \mod 19, 87 \mod 37) = (11, 13)$
  – $51 \mod 703 = (51 \mod 19, 51 \mod 37) = (13, 14)$

• Addition
  – $(87 + 51) \mod 703 = 138 \mod 703$
  – $(11, 13) + (13, 14) = (24 \mod 19, 27 \mod 37) = (5, 27)$
    check $138 \mod 703 = (138 \mod 19, 138 \mod 37) = (5, 27)$

• Multiplication
  – $(87 * 51) \mod 703 = 4437 \mod 703 = 219$
  – $(11, 13) * (13, 14) = (143 \mod 19, 182 \mod 37) = (10, 34)$
    check $219 \mod 703 = (219 \mod 19, 219 \mod 37) = (10, 34)$
Group Work

• Consider 78 mod 703 and 51 mod 703
• Convert these to ordered pairs, perform multiplication, and convert results back to $\mathbb{Z}_{703}$
A Bit of History

- Around 100 AD Sun-Tsu solved the following
  - Find those integers that leave remainders 2, 3, 2 when divided by 3, 5, 7 respectively
  - all solutions have the form 23 + 105 x
  - in general, the CRT finds a correspondence between a system of equations modulo pairwise relatively prime moduli (3, 5, 7) and an equation modulo their product (105)

- This characterization of solving simultaneous modular linear equations is mathematically equivalent to the approach we have presented
## Powers of an Integer

- Here are the powers of integers mod 19

<table>
<thead>
<tr>
<th>a</th>
<th>a^2</th>
<th>a^3</th>
<th>a^4</th>
<th>a^5</th>
<th>a^6</th>
<th>a^7</th>
<th>a^8</th>
<th>a^9</th>
<th>a^{10}</th>
<th>a^{11}</th>
<th>a^{12}</th>
<th>a^{13}</th>
<th>a^{14}</th>
<th>a^{15}</th>
<th>a^{16}</th>
<th>a^{17}</th>
<th>a^{18}</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>13</td>
<td>7</td>
<td>14</td>
<td>9</td>
<td>18</td>
<td>17</td>
<td>15</td>
<td>11</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>8</td>
<td>5</td>
<td>15</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>18</td>
<td>16</td>
<td>10</td>
<td>11</td>
<td>14</td>
<td>4</td>
<td>12</td>
<td>17</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>11</td>
<td>17</td>
<td>9</td>
<td>7</td>
<td>16</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>17</td>
<td>9</td>
<td>7</td>
<td>16</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>9</td>
<td>16</td>
<td>1</td>
<td>6</td>
<td>17</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>9</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td>1</td>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>12</td>
<td>6</td>
<td>3</td>
<td>11</td>
<td>15</td>
<td>17</td>
<td>18</td>
<td>9</td>
<td>14</td>
<td>7</td>
<td>13</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>17</td>
<td>12</td>
<td>4</td>
<td>14</td>
<td>11</td>
<td>10</td>
<td>16</td>
<td>18</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>15</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>8</td>
<td>17</td>
<td>10</td>
<td>7</td>
<td>3</td>
<td>4</td>
<td>18</td>
<td>5</td>
<td>13</td>
<td>11</td>
<td>2</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>12</td>
<td>9</td>
<td>2</td>
<td>11</td>
<td>13</td>
<td>5</td>
<td>18</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>10</td>
<td>17</td>
<td>8</td>
<td>6</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td>1</td>
<td>16</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>11</td>
<td>16</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>1</td>
<td>17</td>
<td>4</td>
<td>11</td>
<td>16</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>
Primitive Roots

• Powers modulo 19
  – In general if $p$ is prime then $a$ is a primitive root of $p$ if $a, a^2, \ldots, a^{p-1}$ are unique
  – the primitive roots of $p = 19$ are 2, 3, 10, 13, 14, 15

• Not all integers are primitive roots
  – All primitive roots have the form $2, 4, p^a, \text{ and } 2p^a$
  – Where $p$ is an odd prime and $a$ is a positive integer
Group Work

• Find all primitive roots of 25
Indices

• Relationship to logarithms
  – Logs are the inverse of exponentiation, for real numbers
    \[ y = x^{\log_x y} \]
  – Indices are the discrete equivalent to logs

• Definitions
  – Recall primitive roots generate 1 to p-1 uniquely
  – For any b there is an i such that \( b \equiv a^i \) mod p
  – This is denoted \( \text{ind}_{a,p}(b) \)
  – \( \text{ind}_{a,p}(1) = 0 \), why?
  – \( \text{ind}_{a,p}(a) = 1 \), why?
Group Work

• Let $p = 7$, what are the primitive roots?

• List all indices for $a = 3$ ordered by the index

• List all indices for $a = 5$ ordered by the number
Some Properties

• Based on Euler’s theorem
  \[ a^z \equiv a^q \mod n \quad \text{if} \quad z = q \mod \phi(n) \]

• Multiplication
  \[ \text{ind}_{a,p}(xy) \equiv \left[ \text{ind}_{a,p}(x) + \text{ind}_{a,p}(y) \right] \mod \phi(p) \]

• Exponentiation
  \[ \text{ind}_{a,p}(y^r) \equiv \left[ r \times \text{ind}_{a,p}(y) \right] \mod \phi(p) \]
# Examples of Discrete Logs

(a) Discrete logarithms to the base 2, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{2,19}(a)$</td>
<td>18</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>16</td>
<td>14</td>
<td>6</td>
<td>3</td>
<td>8</td>
<td>17</td>
<td>12</td>
<td>15</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>4</td>
<td>10</td>
<td>9</td>
</tr>
</tbody>
</table>

(b) Discrete logarithms to the base 3, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{3,19}(a)$</td>
<td>18</td>
<td>7</td>
<td>1</td>
<td>14</td>
<td>4</td>
<td>8</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>11</td>
<td>12</td>
<td>15</td>
<td>17</td>
<td>13</td>
<td>5</td>
<td>10</td>
<td>16</td>
<td>9</td>
</tr>
</tbody>
</table>

(c) Discrete logarithms to the base 10, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{10,19}(a)$</td>
<td>18</td>
<td>17</td>
<td>5</td>
<td>16</td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>15</td>
<td>10</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>14</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

(d) Discrete logarithms to the base 13, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{13,19}(a)$</td>
<td>18</td>
<td>11</td>
<td>17</td>
<td>4</td>
<td>14</td>
<td>10</td>
<td>12</td>
<td>15</td>
<td>16</td>
<td>7</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>13</td>
<td>8</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>

(e) Discrete logarithms to the base 14, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{14,19}(a)$</td>
<td>18</td>
<td>13</td>
<td>7</td>
<td>8</td>
<td>10</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>14</td>
<td>5</td>
<td>12</td>
<td>15</td>
<td>11</td>
<td>1</td>
<td>17</td>
<td>16</td>
<td>14</td>
<td>9</td>
</tr>
</tbody>
</table>

(f) Discrete logarithms to the base 15, modulo 19

<table>
<thead>
<tr>
<th>a</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Ind}_{15,19}(a)$</td>
<td>18</td>
<td>5</td>
<td>11</td>
<td>10</td>
<td>8</td>
<td>16</td>
<td>12</td>
<td>15</td>
<td>4</td>
<td>13</td>
<td>6</td>
<td>3</td>
<td>7</td>
<td>17</td>
<td>1</td>
<td>2</td>
<td>12</td>
<td>9</td>
</tr>
</tbody>
</table>
Why Study Discrete Logs?

• Consider the equation
  – \( y = g^x \mod p \)
  – If \( g, x, \) and \( p \) are known, then it is easy to compute \( y \)
  – But if \( g, y, \) and \( p \) are known and are large numbers, it is almost impossible to compute \( x \) in a reasonable amount of time

• Where are they used
  – The Diffie-Hellman key exchange algorithm
  – The elliptic curve public key cryptography system