Announcements

• Today is the 21st day of the 21st year of the 21st century
Primality Testing

• Miller-Rabin test demonstrated importance of randomized algorithm
  • Break through result in 1980
• Depends on number theory (maybe a senior ugrad class)
  • But much of the algorithm can be appreciated without the theory
• The key concept is that of a witness
  • If something is true, a witness always says TRUE
  • If something is false, a witness says TRUE with probability less than ½
Primality testing

Is the number:
38,448,590,786,041,766,459,732,220,363,801,744,241,896,763,259,493,887,920,989,231,800,007,262,253,532,084,767,190,
7,441,618,354,889,045,484,455,604,450,713,181,265,743,757,650,808,578,235,094,058,535,442,090,523,274,067,570,229,4
06,671,451,796,017,542,179,880,527,768,546,296,447,905,493,082,191
prime?

• A number \( p \) is prime if its only proper divisors are 1 and \( p \), and is composite otherwise

• Small primes \( \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots \} \)

• Simple primality testing algorithms
  • Trial division
  • Sieve of Eratosthenes
Why prime testing is important: cryptography

• RSA public key encryption
  • Relies on factoring “being hard”, $N = pq$ where $p$ and $q$ are prime
  • Recommendation is that $N$ is 2048 bits with $p$ and $q$ roughly 1024 bits
  • 1024 bits is roughly 300 digits

• Need a way to generate “random primes”
  • Guess and check
Complexity of number problems

• Run time based on size of input
• Input N has size $\log_2 N$
• Polynomial time corresponds to polynomial in the size of the number
• Runtime polynomial in N is exponential in the number of bits
Bignum computation

- Arithmetic computation on large numbers – hundreds or thousands or millions of digits
- Run time expressed as a function of the number of digits
- Addition of two n-bit numbers: $O(n)$
- Multiplication of two n-bit numbers: $O(n^2)$ or $O(n^{3/2})$ or $O(n \log n \log \log n)$
- Bignum arithmetic implemented by storing numbers in an array of ints
  - 1024 bit number would require an array of 32 ints
Exponentiation: Compute $A^N$

• Do the computation mod $M$
  • $129038105814095380935^{8430981423091243809}$ MOD 10000000000000000000000

• Compute by repeated squaring

• $A$ raised to $2^K$ can be computed in $K$ multiplications
Greatest Common Divisor

- GCD(A, B) = D, where D is the largest number that divides both A and B
- Runs in O(n^2) time for n bit numbers

```python
function gcd(a, b)
    while b ≠ 0
        t := b
        b := a mod b
        a := t
    return a
```

A: 33707, B: 15207
A: 15207, B: 3293
A: 3293, B: 2035
A: 2035, B: 1258
A: 1258, B: 777
A: 777, B: 481
A: 481, B: 296
A: 296, B: 185
A: 185, B: 111
A: 111, B: 74
A: 74, B: 37
A: 37, B: 0
Prime testing – Idea: Modular arithmetic

• Let $P$ be prime
• Consider the set of integers \{1, 2, 3, \ldots, P-1\} with the operation $\ast$, where multiplication is done mod $P$
• Can the structure of modular multiplication be used to show $P$ is prime?
• Set with multiplication mod $P$ referred to as $\mathbb{Z}_P^*$
Modular multiplication

<table>
<thead>
<tr>
<th></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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>1</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>6</td>
<td>11</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>11</td>
<td>4</td>
<td>10</td>
<td>3</td>
<td>9</td>
<td>2</td>
<td>8</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>14</td>
<td>8</td>
<td>2</td>
<td>9</td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>11</td>
<td>5</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>3</td>
<td>11</td>
<td>6</td>
<td>1</td>
<td>9</td>
<td>4</td>
<td>12</td>
<td>7</td>
<td>2</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td>12</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>11</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>12</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>3</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>6</td>
<td>11</td>
<td>3</td>
<td>8</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>14</td>
<td>6</td>
<td>13</td>
<td>5</td>
<td>12</td>
<td>4</td>
<td>11</td>
<td>3</td>
<td>10</td>
<td>2</td>
<td>9</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>1</td>
<td>9</td>
<td>2</td>
<td>10</td>
<td>3</td>
<td>11</td>
<td>4</td>
<td>12</td>
<td>5</td>
<td>13</td>
<td>6</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>6</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>6</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td>14</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>13</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>12</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>14</td>
<td>12</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Zero divisors for integers mod N

• X is a zero divisor if AX = 0 mod N for some A != 0
• Fact: X is a zero divisor if and only if GCD(X, N) > 1

• \( Z^*_N = \{ y \in [1 .. N-1] \mid \text{GCD}(y, N) = 1 \} \)
• \( |Z^*_N| = \Phi(N) \)
Powers of elements

• Compute $A^1, A^2, A^3, \ldots, A^{p-1}$

\[ P = 7, 11, 13 \]
|   | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 | 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 |
| 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 |
| 5 | 8 | 6 | 13 | 14 | 2 | 10 | 16 | 12 | 9 | 11 | 4 | 3 | 15 | 7 | 1 |
| 6 | 2 | 12 | 4 | 7 | 8 | 14 | 16 | 11 | 5 | 10 | 3 | 9 | 6 | 12 | 4 |
| 7 | 15 | 3 | 4 | 11 | 9 | 12 | 16 | 10 | 2 | 14 | 13 | 6 | 8 | 5 | 1 |
| 8 | 13 | 2 | 16 | 9 | 4 | 15 | 1 | 8 | 2 | 16 | 9 | 4 | 15 | 1 | 8 |
| 9 | 15 | 14 | 16 | 8 | 4 | 2 | 1 | 9 | 13 | 15 | 16 | 8 | 4 | 2 | 1 |
| 10 | 15 | 14 | 16 | 8 | 4 | 2 | 1 | 9 | 13 | 15 | 16 | 8 | 4 | 2 | 1 |
| 11 | 2 | 5 | 4 | 10 | 8 | 3 | 16 | 15 | 13 | 7 | 9 | 4 | 15 | 1 |
| 12 | 8 | 11 | 13 | 3 | 2 | 7 | 5 | 16 | 9 | 6 | 5 | 14 | 10 | 15 |
| 13 | 16 | 4 | 1 | 13 | 6 | 4 | 1 | 13 | 6 | 4 | 1 | 13 | 6 | 4 |
| 14 | 9 | 7 | 13 | 12 | 15 | 6 | 16 | 3 | 8 | 10 | 4 | 5 | 2 | 11 | 1 |
| 15 | 4 | 9 | 16 | 2 | 13 | 8 | 11 | 5 | 16 | 2 | 13 | 8 | 11 | 5 |
| 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 |

$P = 17, 19, 23$
<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>7</th>
<th>5</th>
<th>1</th>
<th>2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

$P = 9, 12, 15, 21$
\( P = 9, 12, 15, 21 \)

\( Z^*_N \)
Idea (that doesn’t quite work)

• Theorem: if P is prime, $A^{P-1} = 1 \pmod{P}$
• Pick a bunch of numbers at random from $[1 \ldots P-1]$
  • Compute $X^{P-1} \pmod{P}$ for each one
  • If all results are 1, then say Prime
  • If at least one of them is not 1, then say Composite
Carmichael Numbers
What about $561 = 3 \cdot 11 \cdot 17$

- $2^{560} = 1 \mod 561$
- $4^{560} = 1 \mod 561$
- $5^{560} = 1 \mod 561$
- $7^{560} = 1 \mod 561$
- $8^{560} = 1 \mod 561$
- $10^{560} = 1 \mod 561$
- $14^{560} = 1 \mod 561$
- \ldots

- Carmichael numbers are rare (but there are an infinite number)
- Either all numbers in $\mathbb{Z}^*_N$ satisfy $X^{N-1} = 1 \mod N$ or at most half the numbers in $\mathbb{Z}^*_N$ satisfy $X^{N-1} = 1 \mod N$
Witnesses and Certificates

• Certificate C that can be used to prove a property
  • To show N is composite, find a number A such that $1 < \text{GCD}(A, N) < N$
  • 178 is a Certificate that 11481 is composite

• Is there a certificate for primality?

• Prime Witness
  • A property that always holds for primes
  • A property that only sometimes holds for composites
Euler Test

• $N - 1 \mod N = -1 \mod N$, so we can think of $N-1$ as $-1$ in $\mathbb{Z}_{N}^{*}$

• For $P$ prime, $a^{(p-1)/2} = 1$ or $a^{(p-1)/2} = -1$
  • Half of the values of $a$ have $a^{(p-1)/2} = 1$ and half have $a^{(p-1)/2} = -1$

• But there are composite numbers that fool the Euler Test
  • $1729 = 7 \times 13 \times 19$
  • $2^{864} = 1 \mod 1729, 3^{864} = 1 \mod 1729, 4^{864} = 1 \mod 1729, \ldots$
Lemma 14.32 (Motwani-Raghavan)

- Let \( N \) an odd composite that is not a power of a prime and suppose that for some \( a \) in \( \mathbb{Z}_N^* \), \( a^{(N-1)/2} = -1 \mod N \)

- Let \( S \) be the set of numbers \( a \) in \( \mathbb{Z}_N^* \) where \( a^{(N-1)/2} = -1 \mod N \) or \( a^{(N-1)/2} = 1 \mod N \)

- Then \( |S| \leq \frac{1}{2} |\mathbb{Z}_N^*| \)

- Or in English: if the Euler Test passes with a -1, then at most half the values fool the test
Prime Testing Algorithm

1. If \( N \) is perfect power return Composite
2. Choose a bunch of random values \( b_1, b_2, \ldots, b_t \) from \([1..n-1]\)
3. If \( \text{GCD}(b_j,N) \) return Composite
4. \( r_j = b_j^{(N-1)/2} \)
5. If \( r_j \neq 1 \) and \( r_j \neq -1 \) return Composite
6. If \( r_j = 1 \) for all \( j \) return Composite
7. Return prime
What could go wrong

• Composite number could fail line 5 and fail line 6 and be called prime

• Prime could be reported as composite on line 6

• Double sided error with failure probability $2^{-t}$
Miller-Rabin test

• Determine if n is prime

• Given an integer a, 1 < a < n,
  • Miller(n, a) returns either “maybe prime” or “definitely composite”
  • For n prime, Miller(n, a) always says “maybe prime”
  • For n composite, Miller(n, a) says “maybe prime” with probability at most ¼ for a random a

• By running the Miller test repeatedly, we can make it arbitrary high probability
Fermat Test

• Fermat’s little theorem
  • For prime \( n \), \( a^{(n-1)} = 1 \pmod{n} \) for all \( a \)

• For most composite numbers, this fails most of the time

• Unfortunately, there are set of composite numbers (Carmichael numbers) that satisfy this
  • \{561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153, \...\}
Miller-Rabin test

• For a prime number $n$, the only square roots of $1$ modulo $n$, are $1$ and $-1$
• For $n = 2^s d + 1$, $a^d \equiv 1 \pmod{n}$ or $a^{(2^r)d} \equiv -1 \pmod{n}$ for some $0 \leq r < s$
• For a composite number at most $\frac{1}{4}$ of values $a$ satisfy these conditions
Pseudo-code

Input #1: $n > 3$, an odd integer to be tested for primality
Input #2: $k$, the number of rounds of testing to perform
Output: “composite” if $n$ is found to be composite, “probably prime” otherwise

write $n$ as $2^r \cdot d + 1$ with $d$ odd (by factoring out powers of 2 from $n - 1$)
WitnessLoop: repeat $k$ times:
    pick a random integer $a$ in the range $[2, n - 2]$
    $x \leftarrow a^d \mod n$
    if $x = 1$ or $x = n - 1$ then
        continue WitnessLoop
    repeat $r - 1$ times:
        $x \leftarrow x^2 \mod n$
        if $x = n - 1$ then
            continue WitnessLoop
    return “composite”
return “probably prime”
Other facts on Prime Testing

• Miller-Rabin test is deterministic if Extended Riemann Hypothesis is true

• 2002 a deterministic polynomial time test based on Cyclotomic Polynomials was discovered
  • Agrawal-Kayal-Saxena, IIT Kanpur
  • Not practical (termed galactic algorithm – see Wikipedia)

• Factoring is thought to be harder then primality testing
  • In practice, numbers of about 100 decimal digits are factorable in a few hours on a PC
  • 250 decimal digit (829 bit) RSA keys have been factored (2700 CPU Years)
  • Recommendation for RSA is 2048 bit keys
RSA

• RSA key is a number \( n=pq \), where \( p \) and \( q \) are prime
• How do you generate random primes of 300 digits?
  • Generate random number of 300 digits and test if they are prime
  • Of course, there are simple tricks to avoid small divisors
• Prime number theorem: Probability of a random number less than \( N \) is prime is about \( 1/\log N \) (Natural logarithm)
• For 300 digits, this is about 1 in 690