Evan Heaton : CS315 : Homework 5 (BONUS) : 11/9/2015

1. Generating random binary numbers is easy, and you can view my implementation of it in the attached code. It's important to seed the pseudo-random number generator with the current time, so that the program will generate different numbers each time it is run.

2. The method to compute modular exponentiation was created in a previous homework assignment, and was simply copied over for re-use in this assignment.

3. The method to test for primality is simply an instance of modular exponentiation. To see if the result vector is equal to 1, check if the size of the vector is 1, and that number at the first index is 1.

Important notes:

My algorithm for detecting prime numbers using modular arithmetic only failed 1 out of 100 times. This is in accordance with Fermat's Little Theorem and Miller/Rabin's prime number test, which limits the error of said method by ¼.

We are generating random numbers in the set $\{2^{n-1} \dots 2^n\}$ because the first bit is always 1. Let's find the total number of primes in that range by first finding the number of primes in the larger range $\{0 \dots 2^n\}$ and subtracting the primes from the range $\{0 \dots 2^{n-1}\}$

$$primes\ in\ range\ \{0 \dots x\ with\ n\ bits\} = \frac{1}{ln(2)} * \frac{2^n}{n}$$

so, the total number of primes in range $\{2^{n-1} \dots 2^n\}$ is about 5909.278887 - 3151.615407 = 2757.66348.

Divide this number by the 2^{n-1}, and you will get 2757.66348 / 2^{15} = 0.0841572107, which represents the likelihood of selecting a prime number at random in the range $\{2^{n-1} \dots 2^n\}$.

Multiply this by 2 because we are only selecting odd numbers in this range and you get 0.1683144214.

Now, take 1 / 0.1683144214 to find the average number of tries it should take to find a prime with that number of bits. For 16 in this instance it would be 5.941261548.

Here's the formula I came up with: $1 / (((\frac{1}{ln(2)} * \frac{2^n}{n} - \frac{1}{ln(2)} * \frac{2^{n-1}}{n-1}) / 2^{n-1}) * 2)$

This yields the following:

for 16 bits: 5.941261548 iterations.
for 32 bits: 11.46003339 iterations.
for 64 bits: 22.53846316 iterations.
for 128 bits: 44.71349431 iterations.

The rest of the pages are output from running my code!

1111010101000111 = 62791
Prime by brute force
1000010010010001 = 33937
Prime by brute force
1011101010101111 = 47791
Prime by brute force
1110010110010011 = 58771
Prime by brute force
1000011110100001 = 34721
Prime by brute force
1010011001011101 = 42589
Prime by brute force
1001000010000101 = 36997
Prime by brute force
1011111000010101 = 48661
Prime by brute force
1111110011101011 = 64747
Prime by brute force
1000110110000101 = 36229
Prime by brute force
1010000100110101 = 41269
Prime by brute force
1010110010010011 = 44179
Prime by brute force
1111010001010101 = 62549
Prime by brute force
1001011100001111 = 38671
Prime by brute force
1000100001010001 = 34897
Prime by brute force
1000100101010111 = 35159
Prime by brute force
1001011000101111 = 38447
Prime by brute force
1110110011000011 = 60611
Prime by brute force
1001100101000111 = 39239
Prime by brute force
1000101000011001 = 35353
Prime by brute force
1000000000010111 = 32791
IS NOT PRIME! due to factor of 11
IS NOT PRIME! due to factor of 121
1001010101001011 = 38219

Prime by brute force
1001101110111101 = 39869
Prime by brute force
1111101100010111 = 64279
Prime by brute force
1010011000000011 = 42499
Prime by brute force
1101110110101011 = 56747
Prime by brute force
1001001010111001 = 37561
Prime by brute force
1000100111000011 = 35267
Prime by brute force
1001001111101111 = 37871
Prime by brute force
1100100000111001 = 51257
Prime by brute force
1110011011100011 = 59107
Prime by brute force
1100100011011101 = 51421
Prime by brute force
1011101010101111 = 47791
Prime by brute force
1010011010110101 = 42677
Prime by brute force
1110000101100001 = 57697
Prime by brute force
1111110111100101 = 64997
Prime by brute force
1001110010111011 = 40123
Prime by brute force
1011101011110001 = 47857
Prime by brute force
1000111001100011 = 36451
Prime by brute force
1010010101011011 = 42331
Prime by brute force
1111111001011111 = 65119
Prime by brute force
1100010001110011 = 50291
Prime by brute force
1010010110100111 = 42407
Prime by brute force
1001001011000101 = 37573

Prime by brute force
1000001101010111 = 33623
Prime by brute force
1011100011000111 = 47303
Prime by brute force
1010001001111001 = 41593
Prime by brute force
1101100101110011 = 55667
Prime by brute force
1001010101001011 = 38219
Prime by brute force
1100101011011001 = 51929
Prime by brute force
1000011100011111 = 34591
Prime by brute force
1010001110100101 = 41893
Prime by brute force
1001011010101001 = 38569
Prime by brute force
1101100110010001 = 55697
Prime by brute force
1111101010101011 = 64171
Prime by brute force
1100000111001101 = 49613
Prime by brute force
1011001011010011 = 45779
Prime by brute force
1001010111100011 = 38371
Prime by brute force
1101110101010011 = 56659
Prime by brute force
1011000011101001 = 45289
Prime by brute force
1100100000010001 = 51217
Prime by brute force
1110110101111001 = 60793
Prime by brute force
1100101111111111 = 52223
Prime by brute force
1111001000011101 = 61981
Prime by brute force
1000010100001001 = 34057
Prime by brute force
1001001010000011 = 37507

Prime by brute force
1001100000001011 = 38923
Prime by brute force
1000100111110101 = 35317
Prime by brute force
1101001001000111 = 53831
Prime by brute force
1100111110110011 = 53171
Prime by brute force
1011100110110111 = 47543
Prime by brute force
1101010100011111 = 54559
Prime by brute force
1000011011101001 = 34537
Prime by brute force
1100101110111001 = 52153
Prime by brute force
1000100100001001 = 35081
Prime by brute force
1010110111000011 = 44483
Prime by brute force
1001100011011101 = 39133
Prime by brute force
1100010101000111 = 50503
Prime by brute force
1011100000000111 = 47111
Prime by brute force
1110010100111111 = 58687
Prime by brute force
1001111111000111 = 40903
Prime by brute force
1101100000110111 = 55351
Prime by brute force
1011000011101101 = 45293
Prime by brute force
1101001000110101 = 53813
Prime by brute force
1110110001101001 = 60521
Prime by brute force
1011000011101001 = 45289
Prime by brute force
1101000000100001 = 53281
Prime by brute force
1011110100010111 = 48407

Prime by brute force
1100011111010101 = 51157
Prime by brute force
1011001100101101 = 45869
Prime by brute force
1001111110001111 = 40847
Prime by brute force
1010010011111111 = 42239
Prime by brute force
1111000001111001 = 61561
Prime by brute force
1110001100101001 = 58153
Prime by brute force
1000011000111111 = 34367
Prime by brute force
1011001010111101 = 45757
Prime by brute force
1110100100111011 = 59707
Prime by brute force
1001001001101011 = 37483
Prime by brute force
1011100101100011 = 47459
Prime by brute force
1011000001001011 = 45131
Prime by brute force

Took 1 iterations to generate prime number with 16 bits <1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1> : <3, 6, 1, 8, 4> : 1011110000100011 : 48163
Took 18 iterations to generate prime number with 32 bits <1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1> : <3, 5, 4, 5, 5, 5, 7, 5, 1, 4> : 11110111110011110100001011111101 : 4157555453
Took 33 iterations to generate prime number with 64 bits <1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1> : <7, 6, 8, 1, 6, 3, 4, 1, 3, 4, 5, 8, 2, 3, 4, 1, 9, 2, 1, 1> : 1001110010110011001110100101101100111110100101010010010000001011 : 11291432854314361867
Took 54 iterations to generate prime number with 128 bits <1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1> : <7, 7, 5, 4, 9, 0, 4, 9, 3, 9, 2, 3, 3, 8, 1, 5, 5, 4, 8, 3, 3, 0, 2, 4, 4, 9, 4, 3, 2, 9, 4, 6, 2, 8, 2, 7, 7, 3, 3> : 11111110000101000001100100001100100101001000111101010011001010111000101010101101111001001101111011110110101111101111000111110001 : 337728264923494420338455183329394094577