TECHNISCHE HOCHSCHULE DEGGENDORF

Selected Topics of Embedded Software Development 2

WS-2021/22

Prof. Dr. Martin Schramm

Testing and generating Prime Numbers and Safe Primes using CryptoCore

Group 2 – Team 4

Rashed Al-Lahaseh – 00821573

Vikas Gunti - 12100861

Supriya Kajla – 12100592

Srijith Krishnan – 22107597

Wannakuwa Nadeesh – 22109097

History Remarks

Fist attempts to find fast primality algorithms were based on **Fermat's Little Theorem** [1] asserting that for prime n and for any positive integer a, the following relation holds

$$a \equiv a \, mod \, n$$

Indeed, many composite integers do not satisfy the formula and can be discarded after the first check.

Composite n that satisfies formula are called Fermat pseudoprimes relative to base a
it is important to note that all strong pseudoprimes relative to base a are also Fermat pseudoprimes relative to a.
We can decrease the number of false decisions by Fermat's test by checking the relation formula with several different a. However, this does not allow us to completely avoid false conclusions since so-called **Carmichael numbers** [2] exist.

1- Fermat primality test

Fermat's little theorem states that if p is prime and a is not divisible by p, then

$$a^{p-1} \equiv 1 \ (mod \ p)$$

If one wants to test whether p is prime, then we can pick random integers a not divisible by p and see whether the equality holds. If the equality does not hold for a value of a, then p is composite.

However, note that for $a \equiv 1 \ (mod \ p)$, the above congruence holds trivially. It also holds trivially if p is odd and $a \equiv -1 \ (mod \ p)$. For this reason, one usually chooses a number a in the interval $1 < a < p - 1$.

Any a such that

$$a^{n-1} \ \equiv 1 \ (mod \ n)$$

when n is composite a is known as a **Fermat liar** (F-Liar). In this case n is called Fermat pseudoprime to base a.

If we do pick an a such that

$$a^{n-1} \ \not\equiv 1 \ (mod \ n)$$

then a is known as a **Fermat witness** (F-witness) for the compositeness of n.

2- Carmichael numbers

Integer n is called a Carmichael number if it satisfies ($a^n \equiv a \ mod \ n$) for all a. Carmichael numbers appear relatively rarely and the least Carmichael number is 561 = 3 x 7 x 11.

Conclusion

A Carmichael number will pass a Fermat primality test to every base n relatively prime to the number, even though it is not actually prime.

This makes tests based on Fermat's Little Theorem less effective than strong probable prime tests such as the Miller–Rabin primality test.

However, no Carmichael number is either a **Euler–Jacobi pseudoprime** [3] or a **Strong pseudoprime** [4] to every base relatively prime to it so, in theory, either a Euler or a strong probable prime test could prove that a Carmichael number is, in fact, composite.

3- Euler-Jacobi pseudoprime

In number theory, an odd integer n is called a Euler–Jacobi probable prime (or, more commonly, a Euler probable prime) to base a, if a and n are coprime, and

$$a^{\frac{n-1}{2}} \equiv \frac{a}{n} \ (mod\ n)\text{; where } \frac{a}{n} \text{ is the Jacobi symbol}$$

If n is an odd composite integer that satisfies the above congruence, then n is called a Euler–Jacobi pseudoprime or, more commonly, a (Euler pseudoprime) to base a.

4- Strong pseudoprime

A strong pseudoprime is a composite number that passes the Miller–Rabin primality test. All prime numbers pass this test, but a small fraction of composites also pass, making them "pseudoprimes".

Unlike the Fermat pseudoprimes, for which there exist numbers that are pseudoprimes to all coprime bases (the Carmichael numbers), there are no composites that are strong pseudoprimes to all bases.

Why Prime Numbers?

It all started when Sophie Germain a French mathematician and who used safe primes to investigate Fermat's Last Theorem.

A safe prime (p) is **safe** when 2p + 1 is also prime.

Thus 13 is a safe prime, as 27 is also prime, but 17 is not as we get 35 for 2x17+1, and which can be factorized.

These primes have been seen as being important when selected prime numbers to be used in the RSA method.
For this, we create a public modulus (N) and which is the multiplication of two large prime numbers (p and q). If these prime numbers are weak, it can make the factorization of N easier.

The first few Sophie Germain primes are
{2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953}

Overall safe primes are used in cryptography, as they are robust against attacks within discrete log methods (such as for the Diffie Hellman methods).

And here the part of our algorithm important takes its part to test primality (Miller Rabin Test).

Conclusion

So as a conclusion Primes are important because the security of many encryption algorithms are based on the fact that it is very fast to multiply two large prime numbers and get the result, while it is extremely computer-intensive to do the reverse.

When you have a number which you know is the product of two primes, finding these two prime numbers is very hard and this problem is called prime factorization and finding an algorithm which does it fast is one of the unsolved problems of computer science.

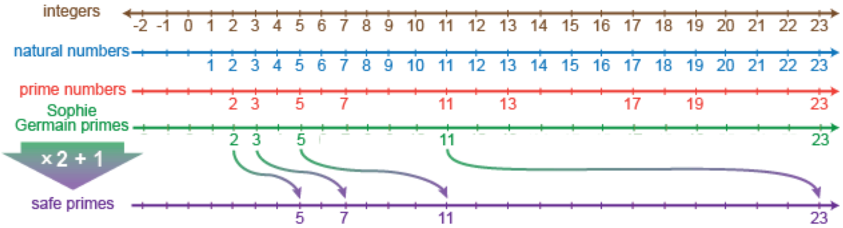


Figure 1: Different Categories of Integer Numbers

Summary of the different categories of integer numbers:

- Integers are the set of negative and positive whole numbers plus zero.

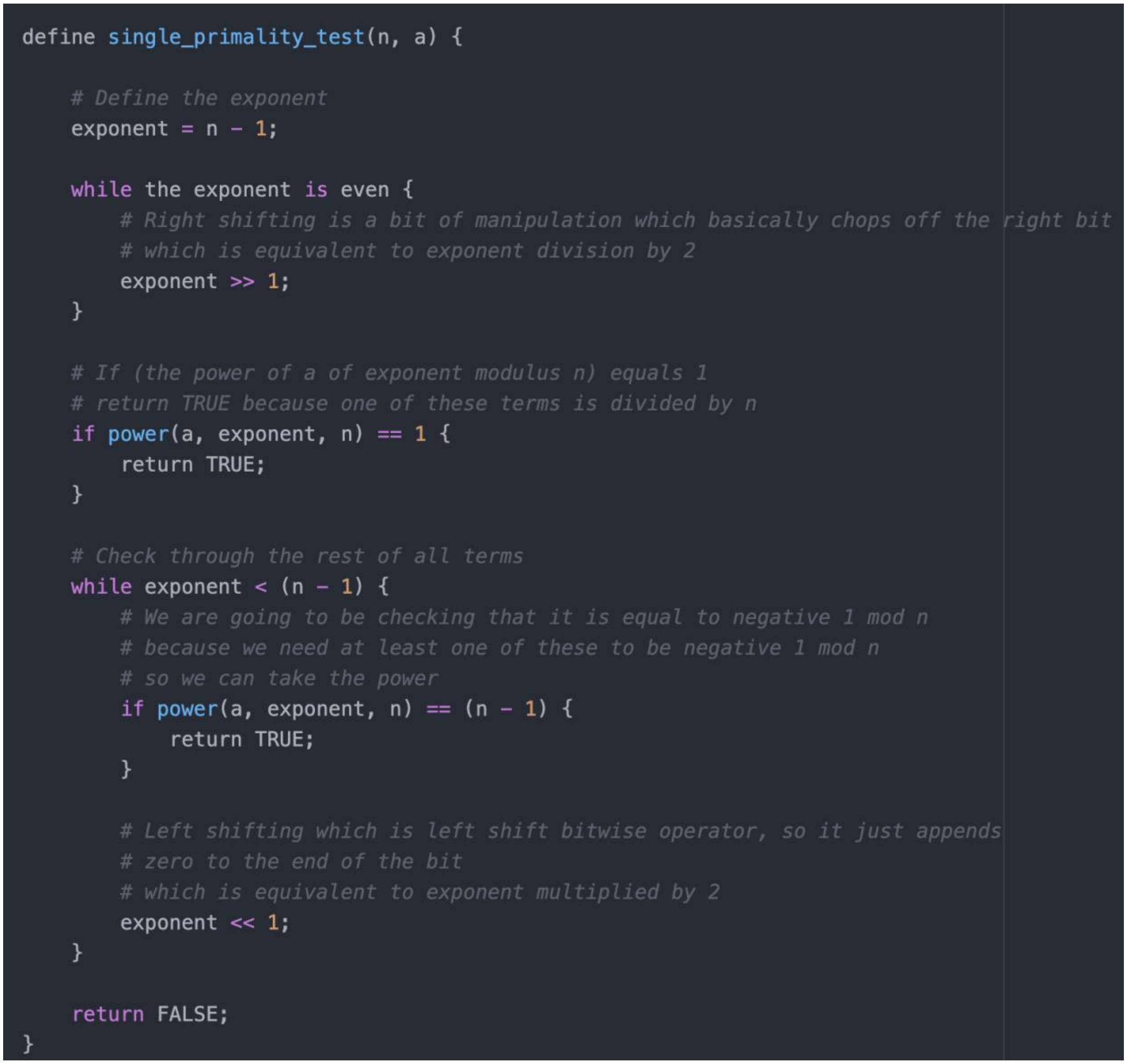
- Natural numbers are integers that are larger than zero (i.e., all positive integers).

- Prime numbers are natural numbers that cannot be divided by any natural numbers other than 1 and itself (i.e., all-natural numbers that have exactly two distinct divisors).

- A Sophie Germain Prime is a prime number that satisfy the following property: when you multiply it by 2 and then add 1, you get another prime number.

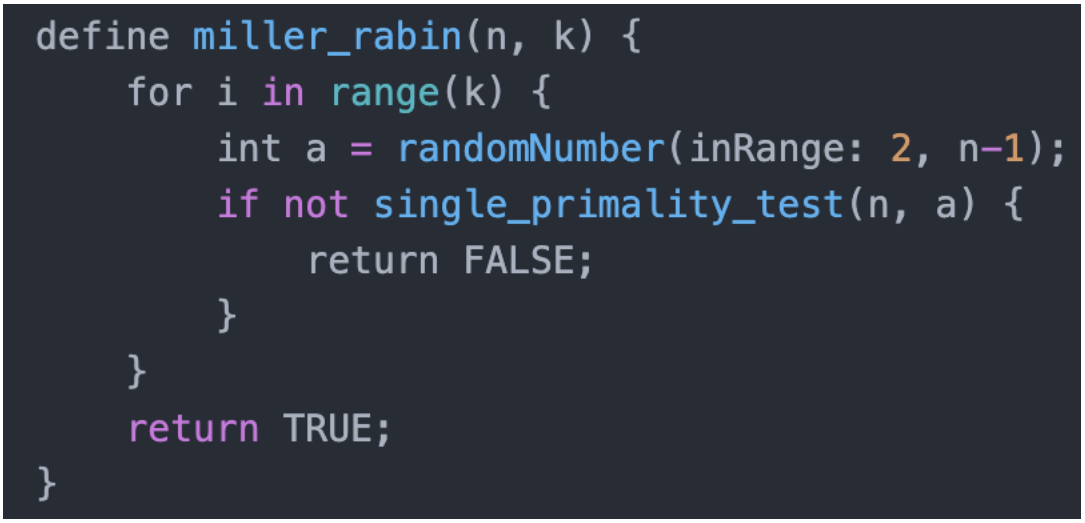
- Finally, the new prime numbers generated in such way are called Safe Primes.

MRT Algorithm



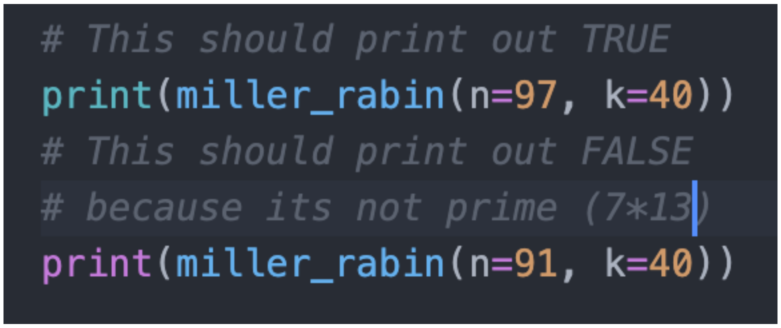
```
define single_primality_test(n, a) {

    # Define the exponent
    exponent = n - 1;

    while the exponent is even {
        # Right shifting is a bit of manipulation which basically chops off the right bit
        # which is equivalent to exponent division by 2
        exponent >> 1;
    }

    # If (the power of a of exponent modulus n) equals 1
    # return TRUE because one of these terms is divided by n
    if power(a, exponent, n) == 1 {
        return TRUE;
    }

    # Check through the rest of all terms
    while exponent < (n - 1) {
        # We are going to be checking that it is equal to negative 1 mod n
        # because we need at least one of these to be negative 1 mod n
        # so we can take the power
        if power(a, exponent, n) == (n - 1) {
            return TRUE;
        }

        # Left shifting which is left shift bitwise operator, so it just appends
        # zero to the end of the bit
        # which is equivalent to exponent multiplied by 2
        exponent << 1;
    }

    return FALSE;
}
```

Figure 2: MRT Pseudocode



```
define miller_rabin(n, k) {
    for i in range(k) {
        int a = randomNumber(inRange: 2, n-1);
        if not single_primality_test(n, a) {
            return FALSE;
        }
    }
    return TRUE;
}
```

Figure 3: MRT Pseudocode



```
# This should print out TRUE
print(miller_rabin(n=97, k=40))
# This should print out FALSE
# because its not prime (7*13)
print(miller_rabin(n=91, k=40))
```

Figure 4: MRT Pseudocode

References

- Wiki: Fermat little theorem
- Wiki: Carmichael number
- Wiki: Euler–Jacobi pseudoprime
- Wiki: Strong pseudoprime
- The Miller-Rabin Test by Martin Dietzfelbinger
- On the Number of Witnesses in the Miller–Rabin Primality Test by Institute of Computational Mathematics and Information Technology, Kazan Federal University
- Sophie Germain Story by Qingbo Wang
- Sophie Germain and Safe Primes by Prof. Bill Buchanan OBE
- Miller-Rabin primality test