2014-08-04-101642

Dr.F.G. Garvan

8/4/2014

Contents

```
## MILLER_RABIN PRIMALITY TEST
def millerrabinv(n,a):
    e = 0
    q = n-1
    c = 0
    m = n-1
    if gcd(a,n) ==1:
        c += 1
    if power_mod(a,m,n) == 1:
        c += 1
    while q % 2 == 0:
        e += 1
        q = q/2
        q = Integer(q)
    if power_mod(a,q,n) == 1:
        c += 1
    for i in range(e):
        if power_mod(a,q*2**i,n) == n-1:
            c += 1
    return c
```

```
millerrabinv(13,2)
```

3

```
millerrabinv(341,2)
```

2

```
factor(341)
```

11 * 31

```
factor(2047)
```

23 * 89

```
millerrabinv(2047,2)
```

3

```
## 2047 is composite but it passes the Miller-Rabin 2-Test
```

```
millerrabinv(2047,3)
```

```
1
```

```
## 2047 does not pass the Miller-Rabin 3-Test
```

```
for n in range(2,5000):
    if millerrabinv(n,2)==3 and not is_prime(n):
        print(n)
```

```
2047
3277
4033
4681
```

```
## The composite numbers less than 5000 that pass the Miller-Rabin 2-Test\
    are
## 2047, 3277, 4033, 4681
for n in range(2,5000):
    if millerrabinv(n,3)==3 and not is_prime(n):
        print(n)
```

```
121
286
703
1891
3281
```

```
## The composite numbers less than 5000 that pass the Miller-Rabin 3-Test\
    are
## 121, 286, 703, 1891, 3281
```