Math 209-16 Homework 4

Due Date: Nov. 1 (TUE), 2022

P1.(3 pts) Use Sage to program the Miller-Rabin test (run $t \geqslant 10$ trials), and use it to investigate which of the following numbers are composite.
(i) $m_1 = 155196355420821961$, (ii) $m_2 = 155196355420821889$,
(iii) $m_3 = 285707540662569884530199015485750433489$.

Solution. Define the function *MillerRabin*(m, t) by Sage in the following:

```
var('m t')
def MillerRabin(m,t):
 i=1;
 j=(m-1).valuation(2);
 d=(m-1)/(2^j);
 while(i>0 and i<=t):
    a=randint(3,m-3);
    if gcd(a,m)!=1:
        i=0;
    else:
        x=mod(a,m)^d;
        if x!=1 and x!=m-1:
            n=1;
            while(n>0 and n<=j-1 and x!=m-1):
                x=mod(x,m)^2;
                if x==1:
                    n=0;
                else:
                    n=n+1;
            if x!=m-1:
                i=0;
        if i>0:
            i=i+1;
 if i==0:
    print(m, "is composite.")
 else:
    print(m, "is a strong probable prime.")
```

By setting $m = m_1, m_2, m_3$ and $t = 100$:

```
MillerRabin(155196355420821961,100)
MillerRabin(155196355420821889,100)
MillerRabin(285707540662569884530199015485750433489,100)
```

we can get the outputs as follows:

```
155196355420821961 is a strong probable prime.
155196355420821889 is composite.
285707540662569884530199015485750433489 is composite.
```

P2.(1 pt) Show that the sequence $1^1, 2^2, 3^3, \ldots,$ considered $\pmod p$ is periodic with least period $p(p-1)$.

Proof. First notice that $(n+p(p-1))^{n+p(p-1)} \equiv n^{n+p(p-1)} \equiv n^n \pmod p$ for any n not divisible by p since $n^{p-1} \equiv 1 \pmod p$, and certainly for n a multiple of p we have $(n+p(p-1))^{n+p(p-1)} \equiv 0 \equiv n^n \pmod p$. Therefore, $p(p-1)$ is indeed a period for the given sequence. Denote the least period of this sequence by k. Then $k \mid p(p-1)$. Since $1^1 \equiv 1 \not\equiv 0 \equiv (1+p-1)^{1+p-1} \pmod p$, we see that $p-1$ is not a period for the sequence and hence $k \nmid (p-1)$. So $p \mid k$, and we may write $k = pt$ for some $t \mid (p-1)$. Now take n to be a primitive root modulo p, we have $n^n \equiv (n+pt)^{n+pt} \equiv n^{n+pt} = n^n \cdot n^{(p-1)t} \cdot n^t \equiv n^n \cdot n^t \pmod p \implies n^t \equiv 1 \pmod p$ and hence $(p-1) \mid t$ since n is a primitive root modulo p. As a consequence, $t = p-1$ and the least period is $p(p-1)$. □

P3.(2 pts) Show that the decimal expansion of $\frac{1}{p}$ has period $p-1$ if and only if 10 is a primitive root of p.

Proof. Note that if the decimal expansion of a rational number $a \in (0,1)$ is $a = 0.\dot{a}_1 \cdots \dot{a}_m$, and let $x = \overline{a_1 \cdots a_m}$ denote the positive integer with digits a_i's. Then $a = x \sum_{i=1}^{\infty} 10^{-im} = \frac{x}{10^m - 1}$. Also notice that if the decimal expansion of $\frac{1}{n}$ does not terminate $\Rightarrow \frac{1}{n} = 0.\dot{a}_1 \cdots \dot{a}_m$. In particular, for $a = \frac{1}{p}$, its decimal expansion has period $m = p-1$ if and only if $p-1$ is the smallest possible value for m such that there exists some $x \in \mathbb{N}$ satisfying $\frac{1}{p} = \frac{x}{10^m - 1}$, namely, the smallest m such that $10^m \equiv 1 \pmod p$ is $p-1$, which says exactly that 10 is a primitive root of p. □

P4.(1 pt) Prove that if p is a prime having the form $4k+3$, and if m is the number of quadratic residues less than $p/2$, then $1 \cdot 3 \cdot 5 \cdots (p-2) \equiv (-1)^{m+k+1} \pmod{p}$, and $2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{m+k} \pmod{p}$.

Proof. We first compute $1 \cdot 3 \cdot 5 \cdots (p-2) = 1 \cdot 3 \cdots (2k+1) \cdot (2k+3) \cdots (4k+1) \equiv 1 \cdot 3 \cdots (2k+1) \cdot (-2k) \cdots (-2) = (-1)^k (2k+1)! \pmod{p}$. Now we want to show $(2k+1)! \equiv (-1)^{m+1} \pmod{p}$. Notice that $(\frac{-1}{p}) = -1$ since $p \equiv 3 \pmod{4}$, and therefore exactly one of a and $p-a$ is a quadratic residue of p for any $a \in \{1, 2, \ldots, \frac{p-1}{2} = 2k+1\}$. Hence, we have

$$\begin{aligned}
(2k+1)! &= \prod_{\substack{a \text{ quadratic residue} \\ a<\frac{p}{2}}} a \cdot \prod_{\substack{b \text{ quadratic nonresidue} \\ b<\frac{p}{2}}} b \\
&\equiv \prod_{\substack{a \text{ quadratic residue} \\ a<\frac{p}{2}}} a \cdot (-1)^{2k+1-m} \cdot \prod_{\substack{b \text{ quadratic residue} \\ b>\frac{p}{2}}} b \\
&= (-1)^{m+1} \cdot \prod_{a \text{ quadratic residue}} a \pmod{p}
\end{aligned}$$

Now it only remains to show that the product of all quadratic residues $\pmod{p}$ is congruent to 1 when $p \equiv 3 \pmod{4}$. This can be seen by noticing that $a \in \{1, 2, \ldots, p-1\}$ is a quadratic residue if and only if its inverse $\pmod{p}$ is, moreover, a equals its inverse precisely when $a = 1$ since -1 is a quadratic nonresidue. This completes the proof of $1 \cdot 3 \cdot 5 \cdots (p-2) \equiv (-1)^{m+k+1} \pmod{p}$. The other congruence follows from this one and Wilson's theorem. $\square$

P5.(2 pts) Let p be an odd prime. Prove that every primitive root of p is a quadratic nonresidue. Prove that every quadratic nonresidue is a primitive root if and only if p is of the form $2^{2^n}+1$ where n is a non-negative integer, that is, if and only if $p = 3$ or p is a Fermat number.

Proof. If g is a primitive root of p then $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, and hence g is a quadratic nonresidue. It follows that every quadratic nonresidue is a primitive root if and only if the number of quadratics nonresidues is equal to that of primitive roots. But there are $\frac{p-1}{2}$ distinct quadratic nonresidues and $\phi(p-1)$ distinct primitive roots, and $\phi(p-1) = \frac{p-1}{2}$ if and only if $p-1$ is a power of 2. Since p is a prime, we see that it holds if and only if p is of the form $2^{2^n}+1$. $\square$

P6.(2 pts) Show that if p and q are primes, $p = 2q+1$, and $0 < m < (p+1)^{1/2}$, then m is a primitive root $\pmod p$ if and only if it is a quadratic nonresidue $\pmod p$.

PROOF. We have shown in the last problem that every primitive root is a quadratic nonresidue, so it remains to prove the sufficiency. Since $p = 2q+1$, the order of $m \pmod p$ can only be $1, 2, q, 2q$. But since m is a quadratic nonresidue, we have $m^{\frac{p-1}{2}} = m^q \equiv -1 \not\equiv 1 \pmod p$. Also, $0 < m < (p+1)^{1/2}$ implies $m^2 \not\equiv 1 \pmod p$ unless $m = 1$, which is not the case since 1 is a quadratic residue. It follows from these two observations that the order of $m \pmod p$ must be $2q$. In other words, m is a primitive root modulo p. $\square$

P7.(2 pts) Prove that there are infinitely many primes of each of the forms $3n+1$ and $3n-1$.

PROOF. If there are only finitely many primes of the form $3n+1$, say $p_1, p_2, \ldots, p_k$. Consider any odd prime divisor p of the number $(p_1p_2\cdots p_k)^2+3$, we have $p \equiv 1 \pmod 3$ since $1 = (\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}(\frac{p}{3}) = (\frac{p}{3})$. But by definition p cannot be equal to any of the p_i's, which is a contradiction.

If there are only finitely many primes of the form $3n+2$, say $q_1, q_2, \ldots, q_l$. Then $(q_1q_2\cdots q_l)^2+1 \equiv 2 \pmod 3$, and hence it must have a prime divisor $q \equiv 2 \pmod 3$, which cannot be equal to any of the q_i's. So again we have a contradiction. $\square$

P8.(2 pts) Show that if $p = 2^{2^n}+1$ is prime then 3 is a primitive root $\pmod p$ and that 5 and 7 are primitive roots provided that $n > 1$.

PROOF. Since $p-1$ is a power of 2, we see that a is a primitive root of p if and only if $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$, in other words a is a quadratic nonresidue. Now by quadratic reciprocity, $(\frac{3}{2^{2^n}+1}) = (\frac{2^{2^n}+1}{3}) = (\frac{2}{3}) = -1$ since $2^{2^n} = 4^{2^{n-1}} \equiv 1 \pmod 3$. When $n > 1$, $(\frac{5}{2^{2^n}+1}) = (\frac{2^{2^n}+1}{5}) = (\frac{4^{2^{n-1}}+1}{5}) = (\frac{2}{5}) = -1$, since $4^{2^{n-1}} \equiv (-1)^{2^{n-1}} \equiv 1 \pmod 5$. Similarly, $(\frac{7}{2^{2^n}+1}) = (\frac{2^{2^n}+1}{7}) = (\frac{3}{7})$ or $(\frac{5}{7})$, since $2^n \equiv 1$ or $2 \pmod 3$ and $2^3 \equiv 1 \pmod 7$. Thus, $(\frac{7}{2^{2^n}+1}) = -1$ as both $(\frac{3}{7})$ and $(\frac{5}{7})$ are equal to -1. $\square$

P9.(2 pts) Suppose that $(ab,p)=1$. Show that the number of solutions (x,y) of the congruence $ax^2+by^2\equiv 1 \pmod p$ is $p-(\frac{-ab}{p})$.

PROOF. Notice that $ax^2+by^2\equiv 1 \pmod p \iff y^2\equiv \bar{b}(1-ax^2) \pmod p$, where $\bar{b}$ denotes the inverse of $b \pmod p$. So for any fixed x, the number of solutions for y is $1+(\frac{\bar{b}(1-ax^2)}{p})$, because there are respectively $2,0$ or 1 solutions for y if $\bar{b}(1-ax^2)$ is a quadratic residue, nonresidue, or is divisible by p. Therefore, the total number of solutions of the original congruence is

$$\sum_{x=0}^{p-1}\left(1+\left(\frac{\bar{b}(1-ax^2)}{p}\right)\right)=p+\left(\frac{-a\bar{b}}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2-\bar{a}}{p}\right)$$

As we know $(\frac{-a\bar{b}}{p})=(\frac{-ab}{p})$, it remains to show $\sum_{x=0}^{p-1}(\frac{x^2-\bar{a}}{p})=-1$. For this we turn to consider another congruence $x^2-y^2\equiv\bar{a} \pmod p$, which is equivalent to $y^2\equiv x^2-\bar{a} \pmod p$, and hence has a total number $\sum_{x=0}^{p-1}\left(1+(\frac{x^2-\bar{a}}{p})\right)=p+\sum_{x=0}^{p-1}(\frac{x^2-\bar{a}}{p})$ of solutions for the same reason as explained above. On the other hand, the pair (x,y) corresponds bijectively to the pair $(u=x+y, v=x-y)$ via $x=\frac{u+v}{2}$ and $y=\frac{u-v}{2}$, and $x^2-y^2\equiv\bar{a}\Leftrightarrow uv\equiv\bar{a}$. It is clear that $uv\equiv\bar{a} \pmod p$ has $p-1$ solutions since for any fixed $v\equiv 1,2,\ldots,p-1 \pmod p$, there is a unique solution $u\equiv\bar{v}\bar{a}$ for u. Hence, we conclude that $p+\sum_{x=0}^{p-1}(\frac{x^2-\bar{a}}{p})=p-1$, and so $\sum_{x=0}^{p-1}(\frac{x^2-\bar{a}}{p})=-1$, which is exactly what we want. $\square$

P10.(3 pts) We call $\mathscr{H}$ a one-half set of reduced residues (mod p) if $\mathscr{H}$ has the property that $h \in \mathscr{H}$ if and only if $-h \notin \mathscr{H}$. Let $\mathscr{H}$ and $\mathscr{K}$ be two complementary one-half sets. Suppose that $(a, p) = 1$. Let ν be the number of $h \in \mathscr{H}$ for which $ah \in \mathscr{K}$. Show that $(-1)^\nu = (\frac{a}{p})$. Show that $a\mathscr{H}$ and $a\mathscr{K}$ are complementary one-half sets. Show that

$$\left(\frac{a}{p}\right) = \prod_{h \in \mathscr{H}} \frac{\sin 2\pi ah/p}{\sin 2\pi h/p}.$$

Proof. By definition, the cardinality of any one-half set is $\frac{p-1}{2}$ because it contains exactly one element in each pair $\{k, p-k\}$, $k = 1, 2, \ldots, \frac{p-1}{2}$. Moreover, since $(a, p) = 1$, the set $a\mathscr{H}$ is also an one-half set, and hence

$$\mathscr{H} = \{ah \mid h \in \mathscr{H}, ah \in \mathscr{H}\} \dot{\bigcup} \{-ah \mid h \in \mathscr{H}, ah \in \mathscr{K}\}.$$

Therefore,

$$\prod_{h \in \mathscr{H}} h = \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{H}} ah\right) \cdot \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{K}} (-ah)\right)$$

then it follows that

$$\begin{aligned}
\prod_{h \in \mathscr{H}} ah &= \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{H}} ah\right) \cdot \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{K}} ah\right) \\
&= \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{H}} ah\right) \cdot (-1)^\nu \cdot \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{K}} (-ah)\right) = (-1)^\nu \cdot \prod_{h \in \mathscr{H}} h.
\end{aligned}$$

Thus, $a^{\frac{p-1}{2}} = (-1)^\nu$, i.e., $(\frac{a}{p}) = (-1)^\nu$.

We already know that both $a\mathscr{H}$ and $a\mathscr{K}$ are one-half sets, it is left to show that they are complementary. Indeed, if $ah = ak$ for some $h \in \mathscr{H}$ and $k \in \mathscr{K}$, then we have $h = k$, contradicting that $\mathscr{H}$ and $\mathscr{K}$ are complementary.

Finally, the last identity also follows from the similar observation:

$$\begin{aligned}
\prod_{h \in \mathscr{H}} \sin 2\pi ah/p &= \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{H}} \sin 2\pi ah/p\right) \cdot (-1)^\nu \cdot \left(\prod_{h \in \mathscr{H}, ah \in \mathscr{K}} \sin -2\pi ah/p\right) \\
&= (-1)^\nu \cdot \prod_{h \in \mathscr{H}} \sin 2\pi h/p,
\end{aligned}$$

hence, $(\frac{a}{p}) = (-1)^\nu = \prod_{h \in \mathscr{H}} \frac{\sin 2\pi ah/p}{\sin 2\pi h/p}$. $\square$