Math 780/780I **Test 3** Name: Answer Key. □

1. Recall that Pick's theorem says that for any lattice polygon, P, the area of P is

$$A(P) = I(P) + \frac{1}{2}B(P) - 1$$

where $I(P)$ is the number of lattice points interior to P, $B(P)$ is the number of lattice points on the boundary of P.

(a) Use this to show that a lattice triangle with area 1/2 has no interior lattice points and exactly 3 lattice points on the boundary. *Hint:* A lattice triangle has at least 3 lattice points on the boundary.

Solution: By Pick's Theorem

$$\begin{aligned} 1/2 = A &= I(P) + \frac{1}{2}B(P) - 1 \\ &\geq \frac{1}{2}B(P) - 1 && \text{(As } I(p) \geq 0) \\ &\geq \frac{1}{2}(3) - 1 && \text{(As } B(p) \geq 3) \\ &= \frac{1}{2}. \end{aligned}$$

The only way that this can start and end with 1/2 is if equality holds in all the inequalities. That is of $I(P) = 0$ and $B(P) = 3$, which is just what we wanted to show. □

(b) Show that a lattice n-gon has area at least $n/2 - 1$. *Hint:* A lattice n-gon has at least n lattice points on the boundary.

Solution: Again we use Pick's Theorem.

$$\begin{aligned} A &= I(P) + \frac{1}{2}B(P) - 1 \\ &\leq \frac{1}{2}B(P) - 1 && \text{(As } 0 \leq I(P)) \\ &\leq \frac{1}{2}n - 1 && \text{(As } n \leq B(p)) \end{aligned}$$

as required. □

2. (a) Define the ***Farey series*** $\mathcal{F}_n$.

Solution: This is the series of fractions $\dfrac{p}{q}$ in lowest terms with $0 \leq \frac{p}{q} \leq 1$, with $q \leq n$ and arranged in increasing order. □

(b) State the basic theorem about consecutive terms $\dfrac{a}{b} < \dfrac{a'}{b'}$ in $\mathcal{F}_n$.

Solution: These terms satisfy $a'b - ab' = 1$.qed

(c) If $\dfrac{r-1}{r} < \dfrac{s-1}{s}$ consecutive terms in $\mathcal{F}_n$, show that r and s are consecutive integers.

Solution: Letting $\frac{a}{b} = \dfrac{r-1}{r} < \dfrac{s-1}{s} = \frac{a'}{b'}$. Then

$$1 = a'b - ab' = (s-1)r - (r-1)s = sr - r - rs + s = s - r.$$

Thus $s = r + 1$ which means that r and s are consecutive. □

3. (a) Define the ***Euler phi function*** ϕ.

Solution: If n is a positive integer, then $\phi(n)$ is the number of elements in the set

$$U(n) = \{k : 1 \le k \le n, \gcd(k, n) = 1\}.$$

□

(b) Give a formula for $\phi(n)$. (There is more than one way to give such a formula, any one that is correct will get full credit.)

Solution: One formula is

$$\phi(n) - n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is over all the primes that divide n.

Anther formula is to write n as a product of powers of distinct primes, that is

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}.$$

Then

$$\phi(n) = \left(p_1^{\ell_1} - p_1^{\ell_1 - 1}\right)\left(p_2^{\ell_2} - p_2^{\ell_2 - 1}\right) \cdots \left(p_k^{\ell_k} - p_k^{\ell_k - 1}\right)$$

□

(c) If n is divisible by the prime 29, show $\phi(n)$ is divisible by 7.

Solution: Let 29^ℓ be the largest power of 29 that divides n, that is $29^\ell \mid n$, but no larger power of 29 divides n. Then $n = 29^\ell k$ where k will have no factor of 29. Thus $\gcd(29, k) = 1$. Then

$$\phi(n) = \phi(29^\ell k) = \phi(29^\ell - 29^{\ell-1})\phi(k) = (29 - 1)29^{\ell-1}\phi(k) = 7 \cdot 429^{\ell-1}\phi(k)$$

which makes it clear that $7 \mid \phi(n)$. □

4. We have shown that if a prime p divides n, then $(p - 1) \mid \phi(n)$. Use this to show that $\phi(n) = 14$ has no solutions.

Solution: If $\phi(n) = 14$ and p is a prime factor of n, then $(p-1)$ divides 14 so that $(p-1) = 1, 2, 7, 14$. Therefore $p = 2, 3, 8, 15$. As 8 and 15 are not prime the only prime factors of n are 2 and 3. Thus $n = 2^a 3^b$ for some a and b. Therefore $\phi(n) = \phi(2^a)\phi(3^b)$. We have $\phi(2^a) = 1$ (when $a = 0$) or $\phi(2^a) = 2^{a-1}$. So the only possible prime factors of $\phi(2^a)$ is 2. Likewise $\phi(3^b) = 1$ (when $b = 0$) and $\phi(3^b = 2 \cdot 3^{b-1})$ when $b \ge 1$. So the only possible prime factors of 3^b are 2 and 3. This implies the only prime factors of $\phi(n) = \phi(2^a)\phi(3^b)$ are 2 and 3. As 14 has a factor of 7 we see it is impossible for $\phi(n) = 14$ to hold. □

5. Find all the rational points on the hyperbola $x^2 - 2y^2 = 1$. *Hint:* One rational point is $(1, 0)$.

Solution: We do our usual substitution of

$$x = 1 + t$$
$$y = 0 + mt = myt.$$

This gives

$$(1 + t)^2 - 2(mt)^2 = (1 - 2m^2)t^2 + 2t + 1 = 1,$$

that is

$$t((1 - 2m^2)t + 2) = 0$$

which gives $t = 0$ and $(1 - 2m^2)t + 2 = 0$. The second of these gives

$$t = \frac{-2}{1 - 2m^2} = \frac{2}{2m^2 - 1}.$$

So

$$x = 1 + t = 1 + \frac{2}{2m^2 - 1} = \frac{2m^2 + 1}{2m^2 - 1}$$
$$y = mt = \frac{2m}{2m^2 - 1}.$$

As m ranges over the rational numbers these give all the ration points on $x^2 - 2y^2 = 1$ other than $(1, 0)$, which corresponds to the solution $t = 0$. □

6. Let n be a positive integer and a an integer with $\gcd(a, n) = 1$.
(a) Define $\operatorname{ord}_n(a)$.

Solution: $\operatorname{ord}_n(a)$ is the smallest positive integer k such that $a^k \equiv 1 \mod n$. □

(b) Define a ***is a primitive element*** mod n.

Solution: a is primitive element iff $\operatorname{ord}_n(a) = \phi(n)$. □

(c) If $\operatorname{ord}_n(a) = 5$ and $a^m \equiv 1 \mod n$, then use the definition of $\operatorname{ord}_n(a)$ and the division algorithm to show that $5 \mid m$.

Solution: We are assume that 5 is the smallest positive integer such that $a^k \equiv 1 \mod n$. Divide 5 into m to get

$$m = 5q + r \qquad \text{where} \qquad 0 \le r \le 4.$$

Then

$$1 \equiv a^m \equiv (a^5)^q a^r \equiv 1^q a^r \equiv a^r \mod n$$

where we have used that $a^5 \equiv 1 \mod n$. But as $r < 5$ the congruence $a^r \equiv 1 \mod n$ can only hold if $r = 0$, as $k = 5$ is the smallest positive integer with with $a^k \equiv 1 \mod n$. Therefore $m = 5q$ which implies that $5 \mid m$ as required. □