Facultad de Ciencias - UNAM

Teoría de Números I **Nombre Completo:** _____
Otoño 2014
Examen parcial 3 (para casa)
December 1, 2014
Tiempo de examen: 42h Número de cuenta: _____

Este examen contiene 3 páginas (incluyendo esta página de inicio) y 4 problemas. Verifica que el examen esté completo. Ingresa toda la información solicitada en la parte superior de esta página, y pon tu número de cuenta en la parte superior de cada página que uses.

- Este examen está diseñado para resolverse en casa, sin embargo, se espera que el estudiante resuelva estos ejercicios sin consultar libros o páginas web.
- Este examen se debe realizar de manera individual.
- Este examen debe ser entregado el día viernes 2014-12-05 a más tardar a las 12am en el salón de clases o al correo electrónico: buendia@im.unam.mx.
- **Presenta la solución del problema de una manera clara y organizada**. Establece claramente tu respuesta. Si el trabajo para llegar a la solución no es claro, se darán pocos o nada de puntos para el reactivo.
- **Respuestas misteriosas o que no muestren el trabajo NO recibirán puntos**. Una respuesta correcta que no esté justificada con los cálculos que llevan a la solución y/o sus explicaciones, NO recibirá crédito. Una respuesta incorrecta pero que muestra los cálculos y explicaciones puede recibir créditos parciales, si éstos son correctos.
- NO escribas en la tabla de la derecha.

Problema	Puntos	Puntuación
1	10	
2	1	
3	1	
4	1	
Total:	13	

1. (10 points) El objetivo de este ejercicio es hacer una prueba elemental de la reciprocidad cuadrática de Gauss. En particular esta prueba muestra que la reciprocidad cuadrática es una consecuencia del teorema chino del residuo y del criterio de Euler. Cada una de las partes en este ejercicio depende de los resultados obtenidos en los incisos previos.

   Denotemos por $\mathbb{Z}_n$ al conjunto de los enteros módulo n, con n un entero positivo y por $\mathbb{Z}_n^*$ as su grupo de unidades. Sean p, q dos números primos impares.

   Consideremos al grupo $G := \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ con multiplicación $*$ definida entrada por entrada. Decimos que dos elementos (a, b) y (x, y) en H están relacionados ($(a, b) \sim (x, y)$), si $(a, b) * (x, y)^{-1} = (ax^{-1}, by^{-1}) = (1, 1)$ o si $(a, b) * (x, y)^{-1} = (-1, -1)$.

   (a) Demuestra que $\sim$ es una relación de equivalencia.

   (b) Demuestra que el conjunto $S := \{(i, j) : i = 1, 2, \ldots, p-1; j = 1, 2, \ldots, (q-1)/2\}$ es un sistema de representantes de las clases de equivalencia. Es decir, que estos elementos no son equivalentes dos a dos y que cualquier par $(a, b) \in G$ es equivalente a algún elemento en S.

   (c) Demuestra que el producto:

$$\pi := \prod_{(i,j)\in S} (i, j) = ((p-1)!^{(q-1)/2}, ((q-1)/2)!^{p-1}).$$

   (d) Demuestra que $(\frac{q-1}{2})!^2 \equiv (-1)^{\frac{q-1}{2}}(q-1)! \pmod{q}$.

   (e) Usando lo anterior demuestra que

$$\pi \sim ((p-1)!^{(q-1)/2}; (q-1)!^{(p-1)/2}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}).$$

   (f) Usando el teorema chino del residuo ($\mathbb{Z}_{pq}^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$), demuestra que el conjunto:

$$T := \{(k \pmod p; k \pmod q) : k = 1, 2, \ldots, (pq-1)/2; (k, pq) = 1\}$$

   es, también, un sistema de representantes de la relación de equivalencia $\sim$.

   (g) Demuestra que el producto de las k tales que $(k, k) \in T$ es:

$$\prod_{k:(k,k)\in T} k = \frac{(\prod_{i=1}^{p-1} i)(\prod_{i=1}^{p-1} p + i)\cdots(\prod_{i=1}^{p-1}((q-1)/2-1)p + i)(\prod_{i=1}^{(p-1)/2} \frac{q-1}{2}p + i)}{1 \cdot q \cdot 2q \cdot \cdots \cdot \frac{p-1}{2}q}$$

$$\equiv \frac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}} \pmod p.$$

   (h) Da una expresión equivalente para este producto módulo q.

   (i) Usa el criterio de Euler, pera demostrar que:

$$\pi \sim ((p-1)!^{(q-1)/2}(q|p); (q-1)!^{(p-1)/2}(p|q))$$

   en donde $(q|p)$ es el símbolo de Legandre.

(j) Comparando las dos expresiones de π demuestra que

$$(1; (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}) \sim ((q|b); (p|q)).$$

De lo anterior, deduce la ley de la Reciprocidad cuadrática de Gauss:

$$(q|p) = ((-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}})(p|q)$$

(toma en cuenta que todos estos números son uno o menos uno y que si $a, b \in \{1, -1\}$ y $a \equiv b \pmod{p} \Longrightarrow a = b$).

2. (1 point) Evalua lo siguientes símbolos de Legandre:
   (a) $(461|773)$.
   (b) $(1234|4567)$.

3. (1 point) Determina si la siguiente ecuacíon cuadrática tiene solución:

$$2x^2 + 5x - 9 \equiv 0 \pmod{101}.$$

4. (1 point) Demuestra que si p es un primo impar, entonces:

$$(-3|p) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 6 \\ -1 & \text{si } p \equiv 5 \pmod 6). \end{cases}$$

Suerte!!