NOMBRE: Raimundo Herrera Sufán PUNTAJE:

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas — 1' 2016

Tarea 6 – Respuesta Pregunta 1

1. PD Si a a tiene un inverso multiplicativo en $\mathbb{Z}_n$, entonces $\gcd(a, n) = 1$.
Si a tiene un inverso multiplicativo, entonces existe un a^{-1} tal que $a^{-1}a \equiv 1$ mod n.
Ahora, partiendo de eso, se tiene, por la definición de módulo:

$$a^{-1}a \equiv 1 \bmod n$$
$$a^{-1}a \bmod n = 1$$

Luego, existe un único par q, r en $\mathbb{Z}$, con $r = a^{-1}a$, tal que

$$nq + 1 = a^{-1}a$$
$$a^{-1}a - nq = 1$$
$$(a^{-1})a + (-q)n = 1$$

Ahora, si se toma $s = a^{-1}$ y $t = -q$, se tiene

$$sa + tn = 1$$

Teniendo lo anterior, junto con identidad de Bézout, que señala que el gcd entre dos números a y b es el mínimo número positivo tal que $sa + tb = \gcd(a, b)$, se tiene que 1 es el máximo comun divisor entre a y n. Esto, porque al encontrar una combinación lineal de a y n que lleve a 1, se tiene que, $0 < \gcd(a, n) \leq 1$, ya que el gcd debe ser positivo.
De ahí como el único entero mayor que cero y menor o igual que 1 es 1, se tiene que el gcd es 1. Por lo que, por Bézout y el desarrollo anterior, se tiene que son primos relativos, ya que su máximo comun divisor es 1.

■

2. PD n y $n-1$ son primos relativos para todo $n \geq 2$.
Por inducción se tiene que el caso base es para $n = 2$, se traduce en:
CB $P(2) : \gcd(2, 1) = 1$
Lo que es cierto, ya que el máximo común divisor entre 2 y 1 es efectivamente 1, por lo que son primos relativos.
Ahora la hipotesis de inducción corresponde a asumir el caso enésimo, esto es:
HI $P(n) : \gcd(n, n-1) = 1$
Y a partir de eso, lo que queda demostrar, es decir, el paso inductivo, corresponde a $P(n) \rightarrow P(n+1)$, esto es:
PI $\gcd(n, n-1) = 1 \rightarrow \gcd(n+1, n) = 1$

Para esto, tomando la hipótesis y operando sobre ella se tiene

$$
\begin{aligned}
&\gcd(n, n-1) = 1 && \text{Por HI} \\
&sn + t(n-1) = 1 && \text{Por Bézout} \\
&sn + tn - t = 1 && \text{Despejando} \\
&sn + 2tn - tn - t = 1 && \text{Sumando } tn \text{ a ambos lados y despejando} \\
&(s+2t)n + (-t)(n+1) = 1 && \text{Agrupando} \\
&s'n + t'(n+1) = 1 && \text{Tomando } s' = s + 2t \text{ y } t' = -t \\
&\gcd(n, n+1) = 1 && \text{Por Bézout}
\end{aligned}
$$

Luego, a partir de la hipótesis de inducción, es posible llegar a lo que se desea demostrar, es decir, que el máximo común divisor entre n y $n+1$ sea 1, por las mismas razones expuestas en **(1.1)**, considerando que al encontrar la combinación lineal que lleve a 1, este será el gcd, y al ser 1 el gcd, entonces son primos relativos.

■

3. PD a y n son primos relativos si, y solo si, a_0 y n son primos relativos donde a_0 es el digito menos significativo de de la representacion $(a)_n$ en base n.
   Para esto, se demostrará utilizando igualdades, de modo que no será necesario demostrar ambas direcciones. Antes de eso, se sabe que la representación $(a)_n$ corresponde a:

$$(a)_n = \sum_{i=0}^{k} a_i n^i = a_0 + a_1 n + a_2 n^2 + a_3 n^3 + \ ... \ + a_k n^k$$

   Luego, lo que se quiere demostrar es que:

$$\gcd(a, n) = 1 \leftrightarrow \gcd(a_0, n) = 1$$

   Entonces, tomando el teorema del algoritmo de euclides, se sabe que $\gcd(a, b) = \gcd(b, a \bmod b)$, para todo $a, b \in \mathbb{Z} - \{0\}$, por lo que:

$$\gcd(a, n) = \gcd(n, a \bmod n)$$

   Volviendo a lo anterior, se tiene que, utilizando la representación en base n de a:

$$
\begin{aligned}
\gcd(a, n) &= \gcd(n, a \bmod n) \\
&= \gcd(n, (a_0 + a_1 n + \ ... \ + a_k n^k) \bmod n) && \text{Sustituyendo} \\
&= \gcd(n, (a_0 \bmod n + a_1 n \bmod n + \ ... \ + a_k n^k \bmod n) \bmod n) && \text{Por distributividad}
\end{aligned}
$$

   Ahora, se sabe que, por distributividad del módulo en el producto,

$$a_i n^i \bmod n = (a_i \bmod n * n^i \bmod n) \bmod n$$

   Y como $n^i \bmod n = 0, \ \forall i > 0$, se tiene que

$$a_i n^i \bmod n = (a_i \bmod n * 0) \bmod n = 0$$

$$
\begin{aligned}
\gcd(a, n) &= \gcd(n, (a_0 \bmod n + 0 + \ ... \ + 0) \bmod n) && \text{Por lo anterior} \\
&= \gcd(n, (a_0 \bmod n) \bmod n) && \text{Sumando} \\
&= \gcd(n, a_0 \bmod n) && \text{Revirtiendo o sacando el módulo} \\
&= \gcd(a_0, n) && \text{Por el teorema, al revés}
\end{aligned}
$$

   De modo que, se demuestra que obtener el gcd entre a y n es exactamente igual a obtener el gcd entre a_0 y n, por lo que si uno de ellos es 1, el otro también lo será.

■

NOMBRE: Raimundo Herrera Sufán PUNTAJE:

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas — 1' 2016

Tarea 6 – Respuesta Pregunta 2

1. ¿Es cierta la afirmación? Demuestre o de un contra-ejemplo, y en caso de dar contra-ejemplo determine una condición adicional para que se cumpla la afirmación, y demuéstrela.
No es cierta la afirmación ya que, por ejemplo:

$$18 \equiv 0 \bmod 9 = 6 * 3 \equiv 0 \bmod 9$$

Pero,

$$6 \not\equiv 0 \bmod 9 \quad \text{y} \quad 3 \not\equiv 0 \bmod 9$$

Ahora, se pide una condición adicional, para que la afirmación se cumpla. Basta con agregar que n sea primo, para que se cumpla la afirmación. Hay que demostrar entonces que si $ab \equiv 0 \bmod n$ y n es primo, entonces $a \equiv 0 \bmod n$ o $b \equiv 0 \bmod n$.

Si n es primo, en particular a y n al igual que b y n son primos relativos entre sí, ya que esto pasa para todos los primos. A menos que sean iguales (a con n o b con n o ambos), pero ese caso es trivial, ya que si son iguales, si bien no habrá inverso, es inmediato que se cumplirá lo pedido, ya que $x = 0 \bmod x$ para todo x. Que sean primos relativos, por lo visto en clases, que es justamente el recíproco de lo demostrado en **(1.1)**, implica que a y b tienen un inverso en $\mathbb{Z}_n$.

Sabiendo lo anterior se tiene que, si $ab \equiv 0 \bmod n$, con a y b primos relativos con n, entonces, considerando el inverso de a, a^{-1}:

$$\begin{aligned}
&ab \equiv 0 \bmod n \\
&a^{-1} * ab \equiv a^{-1} * 0 \bmod n && \text{Multiplicando por el inverso de } a \\
&b \equiv 0 \bmod n && \text{Ya que } a^{-1}a = 1\text{, por definición y } a^{-1}0 = 0
\end{aligned}$$

Análogamente, considerando el inverso de b, b^{-1}, se tiene:

$$\begin{aligned}
&ab \equiv 0 \bmod n \\
&ab * b^{-1} \equiv b^{-1} * 0 \bmod n \\
&a \equiv 0 \bmod n
\end{aligned}$$

Dichas igualdades solo se cumplen en caso de que b o a sean distinto de n, utilizando el inverso, pero de no serlo, como se dijo anteriormente, es el caso trivial.
En ambos casos, a partir de la equivalencia original, utilizando el hecho de que son primos relativos, y por ende tienen inverso, se puede llegar a que, o bien $a \equiv 0 \bmod n$, o $b \equiv 0 \bmod n$, que es exáctamente lo pedido.
Por último, en el caso de que a o b fueran 0, si bien no existiría inverso, la condición se cumple inmediatamente ya que $0 \equiv 0 \bmod n$, para todo n.

■

2. Encuentre todas las soluciones de $x^2 \equiv 1 \pmod{p}$, con $x \in \mathbb{Z}$ y p primo. En primer lugar, para encontrar las soluciones, se puede ver que para todo n, $n+1 \equiv 1 \bmod n$. Por lo que se intentará encontrar soluciones de la forma $\alpha + 1$, donde α, sea algún múltiplo o múltiplos de p, de modo que su módulo respecto a p sea 0, y solo quede el módulo respecto a 1, que siempre es 1.
En segundo lugar, se considera que los primos son positivos y parten desde el 2, por lo que la solución que se dará cumplira para esos casos.
Ahora, considerando lo anterior, es fácil ver que $p+1$ es una solución, ya que:

$$
\begin{aligned}
&(p+1)^2 = p^2 + 2p + 1 && \\
&(p^2 + 2p + 1) \bmod p && \text{Aplicando módulo} \\
&(p^2 \bmod p + 2p \bmod p + 1 \bmod p) \bmod p && \text{Por distributividad} \\
&(0 + 0 + 1 \bmod p) \bmod p && \text{Ya que múltiplos de } p \bmod p \text{ son } 0 \\
&(1) \bmod p && \text{Por distributividad, al revés}
\end{aligned}
$$

Ahora aplicando lo anterior a la ecuación, se tiene que:

$$
\begin{aligned}
x^2 &\equiv 1 \pmod{p} \\
(p+1)^2 &\equiv 1 \pmod{p} \\
1 &\equiv 1 \pmod{p}
\end{aligned}
$$

Que cumple con lo pedido, ahora es fácil ver que considerando que cualquier otra propuesta de solución que tenga a 1 como un término libre, y los demás términos como múltiplos de p, será solución. De ahí que $kp+1$, con $k \in \mathbb{Z}$ es una solución. Ya que el desarrollo de el cuadrado de dicha solución es $(kp)^2 + 2kp + 1$, que cumple con tener a 1 como término libre, y a los demás términos como múltiplos de p. Luego, del mismo modo, al estar considerando un cuadrado, se tiene que $kp-1$,con $k \in \mathbb{Z}$ también satisface la ecuación, ya que ahora el desarrollo es, $(kp)^2 - 2kp + 1$, que es análogo. Dicho lo anterior las soluciones de $x^2 \equiv 1 \pmod{p}$ son:

$$
\begin{aligned}
x_1 &= kp + 1, \ k \in \mathbb{Z} \\
x_2 &= kp - 1, \ k \in \mathbb{Z}
\end{aligned}
$$

3. <u>PD</u> $(n-1)! \equiv (n-1) \pmod{n}$ si, y solo si, n es primo.
Se procede a demostrar ambas direcciones.
($\Rightarrow$) Si $(n-1)! \equiv (n-1) \pmod{n}$
<u>PD</u> n es primo.
Asumiendo que $(n-1)! \equiv (n-1) \pmod{n}$, por contradicción también se asume que n es un número compuesto.
Si n es compuesto, tiene al menos un divisor d en $\{2..\sqrt{n}\}$, tal que d divide a n. Al d ser menor que $\sqrt{n}$, es también es menor que $n-1$, por lo tanto, tiene que estar contenido en $(n-1)!$ ya que por definición de factorial contiene a todos los números entre 1 y $n-1$. Considerando eso, $d \mid n$ y también, por lo explicado, $d \mid (n-1)!$. En otras palabras, comparten un factor comun.

Ahora operando sobre la hipótesis, se tiene que:

$$
\begin{aligned}
(n-1)! &\equiv (n-1) \pmod{n} \\
n - (n-1)! &\equiv 1 \pmod{n}
\end{aligned}
$$

Ahora, por la definición de módulo, se tiene que señalar que existe un q tal que $aq + r = b$, es equivalente a $b \equiv r \pmod{a}$. Entonces, en lo anterior, se tiene que:

$$
\begin{aligned}
&nq + 1 = n - (n-1)! && \text{Con } r = 1, \ b = n - (n-1)! \text{ y } a = n \\
&1 = n - nq - (n-1)! && \text{Despejando} \\
&1 = (1-q)n + (-1)(n-1)! && \text{Agrupando}
\end{aligned}
$$

De lo que, con $s = 1 - q$ y $t = -1$, se llega a que el $\gcd(n, (n-1)!) = 1$, por lo visto en las demostraciones de **1**, es decir por Bézout, de modo que son primos relativos. He aquí la contradicción ya que si son primos relativos, no pueden tener ningún factor en comun, y si n no es primo, como se dijo antes, si tiene al menos un factor en comun d que divide a n y a $(n-1)!$.

($\Leftarrow$) Si n es primo
PD $(n-1)! \equiv (n-1) \pmod{n}$
Asumir que n es primo, implica que en $\mathbb{Z}_n$ no existirán factores primos de n, y que n es primo relativo con todos los elementos de $\mathbb{Z}_n$. Así, al ser primos relativos, por lo visto en clases, es decir, el recíproco de lo demostrado en **(1.1)**, cada elemento tendrá un inverso en $\mathbb{Z}_n$, de modo que para cada $a \in \mathbb{Z}_n$, se tiene que $a^{-1}a \equiv 1 \pmod{n}$ con $a^{-1} \in \mathbb{Z}_n$ igualmente.
Ahora por propiedad de los módulos, se tiene que si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces se tiene $ac \equiv bd \pmod{n}$, de modo que se pueden multiplicar todas las expresiones necesarias, de modo de formar $1 * 2 * 3 ... * (n-2)$. Esto porque $n-1$ tiene por inverso a si mismo, por lo tanto no se considera en dicho producto, porque se repetirían factores.
Entonces, se tiene, por la propiedad anterior:

$$1 * 2 * 3 ... * (n-2) \equiv 1 \pmod{n}$$

Ahora, multiplicando a ambos lados por $n-1$ se tiene que:

$$1 * 2 * 3 ... * (n-2) * (n-1) \equiv (n-1) \pmod{n}$$

$$(n-1)! \equiv (n-1) \pmod{n}$$

Que es justamente lo que se intentaba demostrar.

■