اسم المادة : نظرية الأعداد

تجمع طلبة كلية التكنولوجيا والعلوم التطبيقية - جامعة القدس المفتوحة

acadeclub.com

وُجد هذا الموقع لتسهيل تعلمنا نحن طلبة كلية التكنولوجيا والعلوم التطبيقية وغيرها من خلال توفيروتجميع كتب وملخصات وأسئلة سنوات سابقة للمواد الخاصة بالكلية, بالإضافة لمجموعات خاصة بتواصل الطلاب لكافة المواد:

للوصول للموقع مباشرة اضغط هنا

وفقكم الله في دراستكم وأعانكم عليها ولا تنسوا فلسطين من الدعاء

نهاد
ص 361

الوحدة الرابعة

فيرما الصغرى

أوجد باقي قسمة 2^{50} على 17

$* \; a^{p-1} = 1 \mod p \qquad * \; (a,p) = 1$

$a^p = a \mod p$

الحل:

$2^{17-1} = 2^{16} = 1 \mod 17$

$(2^{16})^3 = 2^{48} = (1)^3 \mod 17$

نضرب طرفا التطابق بـ 2^2

$2^{48} * 2^2 = 2^{50} = 1 * 2^2 \mod 17$

$2^{50} = 4 \mod 17$

باقي قسمة 2^{50} على $17 = 4$

mod 19

مثال آخر: أوجد باقي قسمة 40^{40} على 19

ق.م.أ

$(19, 40) = 1 \qquad * (a,p) = 1 \qquad * \; a^{p-1} = 1 \mod p$

$a^p = a \mod p$

الحل:

$40^{19-1} = 40^{18} = 1 \mod 19$

نربع $(40^{18})^2 = (1)^2 \mod 19$

لازم نكمل حل أكثر من 19

نضرب بـ 40^4

$40^{36} * 40^4 = 40^{40} = (1)^2 * 40^4 \mod 19$

بدنا 40^{40}

الأساسات متشابهة نجمع الأسس

$40 = 2 \mod 19 \Rightarrow 40^4 = 2^4 \mod 19$

$40^{40} = 2^4 = 16 \mod 19$

الوحدة الرابعة

نهاية ص 361

فيرما الصغرى

أوجد باقي قسمة 2^{50} على 17

$* \ a^{p-1} = 1 \mod p \qquad * \ (a,p)=1$

$a^{p} = a \mod p$

الحل :-

$2^{17-1} = 2^{16} = 1 \mod 17$

$(2^{16})^3 = 2^{48} = (1)^3 \mod 17$

نضرب طرفا التطابق بـ 2^2

$2^{48} * 2^2 = 2^{50} = 1 * 2^2 \mod 17$

$2^{50} = 4 \mod 17$

باقي قسمة 2^{50} على $17 = 4$

mod 19

مثال آخر :- أوجد باقي قسمة 40^{40} على 19

P.م.ح

$(19, 40) = 1 \qquad * (a,p)=1 \qquad * \ a^{p-1} = 1 \mod p$

$a^{p} = a \mod p$

الحل :- $40^{19-1} = 40^{18} = 1 \mod 19$

نربع $(40^{18})^2 = (1)^2 \mod 19$ لازم نكمل حل أكبر من 19

نضرب بـ 40^4 $\quad 40^{36} * 40^4 = 40^{40} = (1)^2 * 40^4 \mod 19$

بدنا 40^{40}

الأساسات متشابهة نجمع الأسس

$40 = 2 \mod 19 \Rightarrow 40^4 = 2^4 \mod 19$

$40^{40} = 2^4 = 16 \mod 19$

باقي قسمة 4^{532} على 11^{p} (a = 4)

$a^{p-1} = 1 \bmod p$ ✓ $(a,p)=1$ ✓

فيرما $a^{p} = a \bmod p$ ✓

الحل: $4^{11-1} = 4^{10} = 1 \bmod 11$

قوة 53 $(4^{10})^{53} = (1)^{53} \bmod 11$

ضرب 4^{2} $4^{530} * 4^{2} = 1 * 4^{2} \bmod 11$

$4^{532} = 16 \bmod 11$

أكبر من 11 نكمل حل ✓ $16 = 5 \bmod 11$

$4^{532} = 5 \bmod 11$

أويلر/ويلسون

الشروط $a^{\phi(m)} = 1 \bmod m$

$(a, m) = 1$

مثال 12) 7^{90} بالمقياس 15
صفحة 38

$\phi(15) = 8$

عدد الأعداد $\{2, \ , \ , 7, 11, 13\}$ التي أقل منه

التي ليس لها مع العدد 15 أي قواسم مشتركة من $\{1, 15\}$ $\{1, 4, 8, 14.$

كم عدد = 8 أعداد

$(7, 15) = 1$

الحل: $7^{\phi(15)} = 7^{8} = 1 \bmod 15$

$7^{2} = 4 \bmod 15$ $(7^{8})^{11} * 7^{2} = (1)^{11} * 7^{2} \bmod 15$

$7^{90} = \underline{49} \bmod 15 \longrightarrow = 4 \bmod 15$

أولي / غير أولي ← أويلر

أوجد باقي قسمة العدد $(7)^{1203}$ على 100

$(a,m)=1$ $\qquad$ $a^{\phi(m)} \equiv 1 \mod m$

الحل: $7^{\phi(100)} = 1 \mod 100$ $\qquad$ $(7,100)=1$

$\phi(100) = \phi(2^2)\,\phi(5^2) = (2^2-2^1)(5^2-5^1)$

$= 2 \cdot 20 = 40$

100
4 25
2 2 5 5
أولي أولي أولي أولي

$(7^{40})^{30} = (1)^{30} \mod 100$

$7^{1200} * 7^3 = 1 * 7^3 \mod 100$

$7^{1203} = 7^3 \mod 100$ نكمل حل

$7^{1203} = \overset{343}{43} \mod 100$

مبرهنة ويلسون.

أوجد الباقي لدى قسمة !26 على العدد 29 ← p

$(p-1)! = -1 \mod p$

$28! = -1 \mod 29$

$26! * 27 * 28 = -1 \mod 29$

$26!\,(-2)(-1) = -1 \mod 29$

$15 * (26)!\,2 = -15 \mod 29$

$25 = -4 \mod 29$

$28 = -1 \mod 29$

$27 = -2 \mod 29$

نظير 2 في المقياس 10

$26! = -\overset{6}{15} \mod 29$

$= 14 \mod 29$

نظير 2 عددا نضربه بـ 2 وعندما نقسمه على 29 الباقي 1.

نظير 2 في المقياس 7 $\qquad$ $2*4=8$ والباقي 1

ملاحظة :- $\phi(n)$ ترمز الى عدد الأعداد المنفصلة عن n التي تقل عنه

$\sigma(n)$: ترمز الى مجموع القواسم الموجبة للعدد (n)

$d(n)$: ترمز الى عدد القواسم الموجبة للعدد (n)

* $\phi(p) = p-1$ $\qquad \phi(7) = 6$
* $\sigma(p) = p+1$ $\qquad \sigma(7) = 8$

$d(p^r) = r+1 \longrightarrow d(2^3) = 3+1 = 4$

$\sigma(p^r) = \dfrac{p^{r+1}-1}{p-1} \longrightarrow \sigma(2^3) = \dfrac{2^4-1}{2-1} = 15$

$\phi(p^r) = p^r - p^{r-1} \Rightarrow \phi(2^3) = 2^3 - 2^2 = 4$

التطابق التربيعي :- $x^2 = -33x - 5 \bmod 37$

اوجد مجموعة حل التطابق التالي :-

اولاً : نتأكد إذا إله حل بقسم 37 على 4 إذا باقي القسمة 1 له حل

$x^2 = -1 \bmod p$

$t = \dfrac{(p-1)}{2}$!

ثانياً: بتخلص من معامل x^2 لازم 1

ثالثاً: بستبدل معامل x بعدد يطابقه

$x^2 + 33x + 5 = 0 \bmod 37$

$37 = 1 \bmod 4$

الباقي 1 له حل

$x^2 - 4x + 5 = 0 \bmod 37$

$x^2 - 4x + 4 = -5 + 4 \bmod 37$ | إكمال مربع $(\frac{b}{2})^2$

$(x-2)^2 = -1 \bmod 37$

$x^2 - 8x = 12 \bmod 29$

$7 * 4 = 28$ ١) نقسم 29 على 4 والباقي 1

٢) أتأكد أن له حل معامل x^2 واحد

٣) نبدل معامل x بعدد يطابقه هون سهل 8x يبقى

$$x^2 - 8x = 12 \bmod 29$$

نضيف 16

$$x^2 - 8x + 16 = \underbrace{12 + 16}_{28} \bmod 29$$

عبارة تربيعية

$$(x-4)^2 = -1 \bmod 29$$ اكمال مربع

$$29 = 1 \bmod 4$$

$x^2 = -1 \bmod p$

$x - 4 = t$

$x - 4 = -t$

$t = \left(\frac{p-1}{2}\right)!$

$$t = \left[\left(\frac{29-1}{2}\right)\right]! = 14!$$

العدد المبغر من mod

$10 = -2 \bmod 12$ $x = 4 \pm 14!$

حتى أكمله 12

$9 = \underset{\text{سالب}}{-3} \bmod 12$

$6 = \underset{\text{سالب}}{-6} \bmod 12$

$14 = \underset{\text{موجب}}{2} \bmod 12$

التطابق التربيعي

$x^2 - 2x = 11 \mod \underline{13}$

$x^2 = -1 \mod p \rightarrow t = \left(\frac{p-1}{2}\right)!$

له حل $3*4 = 12$ والباقي 1

2) تقسم على 4 mod

3) معامل x^2 هو 1

أوجد حلول التطابق التربيعي

$(x-1)^2 = 12 = -1 \mod 13$ إكمال مربع

$13 = 1 \mod 4$ وبما أن

$x = -t + 1$
$x = t + 1$ فإن له حلين هما

لكن $t = \left(\frac{p-1}{2}\right)! = 6! = 720$

إذا $x = 721, -719$

للتأكد $(721)^2 - 2(721) - 11 / 13$

صحيح

1) هل له حل بتقسيم على 4

2) معامل $x^2 = 1$

3) إكمال مربع

مثال آخر :- $\underline{3}x^2 + x + 2 = 0 \mod 13$

بضرب طرفي المعادلة بـ 9 نظير العدد 3 بالمقياس 13

ماهو العدد بضربه بـ 3 + نبدل العدد 9 بالعدد -4 المطابق له بالمقياس 13 وكمله 13

$x^2 + 9x + 18 = 0 \mod 13$

$x^2 - 4x + 4 = -14 \mod \underline{13}$ $4+$ $18-$

$(x-2)^2 = -1 \mod 13$ $13 = 1 \mod 4$

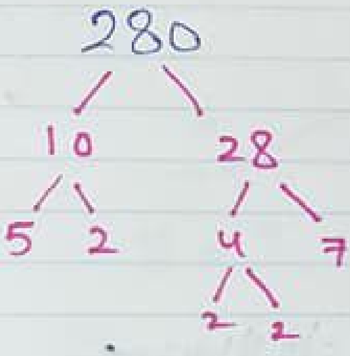
الاقترانات الضربية

$(a, m) = 1$ $\quad a^{\phi(m)} = 1 \mod m.$

عدد الاعداد التي تقل عن m والقاسم المشترك بينها وبين $m = 1$

$d(p^r) = r+1$ $\quad \sigma(p^r) = \frac{p^{r+1}-1}{p-1}$

$\phi(p^r) = p^r - p^{r-1}$



$d(280) = d(2^3)\, d(5^1)\, d(7^1)$

$= (3+1)(1+1)(1+1)$

$= 16$

$\sigma(280) = \left(\frac{2^4-1}{2-1}\right)\left(\frac{5^2-1}{5-1}\right)\left(\frac{7^2-1}{7-1}\right)$

$= 15 * 6 * 8 = 720$

$\phi(280) = (2^3-2^2)(5^1-5^0)(7^1-7^0)$

$= 4 * 5 * 7 = 140$

أول خطوة نحلل لعوامله الأولية

أمثلة

$\phi(45) = (3^2-3^1)(5^1-5^0)$

$= 6 * 4 = 24$

$\phi(192) = (2^6-2^5)(3^1-3^0) = 64$

$\phi(3600) = (2^4-2^3)(3^2-3^1)(5^2-5^1)$

$= 8 * 6 * 20 = 960$

$\phi(p^r) = p^r - p^{r-1}$

$45 = 3^2 * 5$

$192 = 2^6 * 3$

$3600 = 2^4 * 3^2 * 5^2$

$$60 = 2^2 * 5 * 3$$

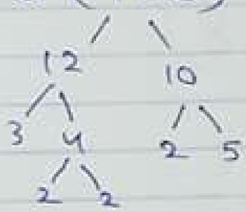
$$\sigma(p^r) = \frac{p^{r+1}-1}{p-1}$$

$$\sigma(60) = \left(\frac{2^3-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$$

$$= 7 * 4 * 6$$

$$= 168$$

$\sigma(120)$



$$120 = 2^3 * 3^1 * 5^1$$

$$= \left(\frac{2^4-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$$

$$= 15 * 4 * 6 = 360$$

مثلثات فيثاغورية

$x = 2st$ $\quad$ $y = s^2 - t^2$ $\quad$ $z = s^2 + t^2$

$(s, t) = 1$ $\quad$ $s > t > 0$

$s = t \mod 2$ واحد زوجي والثاني فردي

جد جميع المثلثات الفيثاغورية البدائية التي طول الوتر فيها يساوي 41

المطلوب :- ايجاد الأزواج (s, t) التي تحقق العلاقات الثلاثة والعلاقة

$z = 41 = s^2 + t^2$

$41 = (1)^2 + (?)^2$ $\quad$ | $\quad$ $41 = (2)^2 + (?)^2$

$41 = (3)^2 + (?)^2$ $\quad$ | $\quad$ $41 = (4)^2 + (?)^2$

$41 = (5)^2 + (?)^2$

مربع العدد الاول يزيد عن نصف العدد

م.م.أ

مربع الأول + مربع الثاني = 41 $\qquad (5,4) = 1$

فردي زوجي

$$41 = (5)^2 + (4)^2$$

$\qquad\quad s \qquad\quad t$

موجبات

احدهما زوجي 4 والآخر فردي 5

$s > t$ تحقق الشروط $5 > 4$

$(5, 4) \qquad s > t > 0$

$$x = 2st$$

$$= 2 \cdot 5 \cdot 4 = 40$$

$$y = s^2 - t^2 = 25 - 16 = 9$$

$$z = s^2 + t^2 = 41$$

أوجد كل المثلثات الفيثاغورية التي طول الوتر فيها 65

نبحث عن (s,t) $\quad z = s^2 + t^2 = 65$

$x = 2st$

$y = s^2 - t^2$

حلان $(\overset{\text{زوجي}}{7}, \underset{\text{فردي}}{4})$, $(\overset{\text{زوجي}}{8}, \underset{\text{فردي}}{1})$

$s = 7$
$t = 4$

$x = 2 \cdot 7 \cdot 4$

$y = 49 - 16$

$z = 49 + 16$

$(16, 63, 65)$, $(56, 33, 65)$

$s > t > 0$ $\quad$ ق.م.أ $= 1$

أوجد كل المثلثات الفيثاغورية التي طول احد الساقين فيها $x = 24$

بما أن $x = 24$ عدد زوجي

x زوجي

y, z فردي

نبحث عن (s,t) التي تحقق الشروط التي أهمها

$x = 2st$

$y = s^2 - t^2$

$z = s^2 + t^2$

نقسم على 2

$\frac{24}{2} = \frac{2st}{2}$

$12 = st$

$s = 1$
$t = 12$