2.

Table des racines primitives etc. pour les nombres premiers depuis 3 jusqu'à 101, precédée d'une note sur le calcul de cette table.

(Par l'éditeur.)

C'est à l'occasion de quelques recherches dans la théorie des nombres, que j'ai calculé une table des racines primitives pour les nombres premiers depuis 3 jusqu'à 101, laquelle ainsi fait suite à celle d'Euler qui contient les racines primitives depuis 3 jusqu'à 37. Comme le calcul, que j'ai fait, donna en même tems, et comme par lui même, les restes des puissances des nombres naturels divisés par les divers nombres premiers, et en sus les nombres dont les puissances moindres que celles des racines primitives, divisées par les nombres premiers, laissent 1 pour restes, et lesquels l'on pourrait nommer *racines secondaires* ou *racines primitives subordonnées:* ces derniers nombres et les restes des puissances dont les exposans sont diviseurs du nombre premier donné diminué d'une unité, ont été introduits également dans la table.

Je vais présenter ici cette table puisque, une fois calculée, elle pourroit être utile à ceux qui s'occupent de la théorie des nombres et de ses applications dans l'analyse.

Quant au calcul que j'ai employé pour construire la table, il ne repose que sur des théorèmes assez connus; mais comme l'application de ces théorèmes a fourni un mécanisme de calcul remarquable par sa simplicité et par la facilité et sûreté avec lesquelles il a donné, comme d'un seul jet, non seulement les racines primitives cherchées, mais encore les autres nombres remarquables, je ferai précéder la table d'une explication de ce mécanisme du calcul.

Note sur le calcul de la table ci-jointe.

Je commencerai par énoncer en peu de mots les principes qui ont servi de base au calcul. Les personnes bien versées dans la théorie des nombres pourront passer cet énoncé.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

I. Soit p un nombre premier quelconque donné, on sait qu'en vertu du théorème de Fermat, toutes les valeurs 1, 2, 3, 4 .... $p-1$ de a satisfont à l'équation

$$1. \quad a^{p-1} = Np + 1,$$

où N signifie un nombre entier. Quelques unes de ces valeurs de a, élevées successivement à toutes les puissances 2, 3, 4, 5mes etc., et ces puissances divisées ensuite par p, laissent pour restes des nombres différents de 1, et ne présentent pas ce dernier reste avant la puissance $p-1^{me}$, de sorte que dans l'équation

$$2. \quad a^x = Np + 1,$$

la *moindre* valeur de x est $p-1$. Ces valeurs de a sont celles qu'on nomme *racines primitives.*

II. Mais, si τ exprime les divers diviseurs premiers de $p-1$, de sorte que p. ex.

$$3. \quad \tau\lambda = p-1:$$

il y a toujours et pour chaque τ des valeurs de a parmi celles 1, 2, 3, ... $p-1$ qui satisfont déjà à l'équation

$$4. \quad a^\tau = Np + 1,$$

sous condition que τ est le *moindre* exposant de la puissance de a, laquelle, divisée par p, laisse 1 pour reste. Ces valeurs de a sont celles qu'on pourrait nommer *racines secondaires*, ou *racines primitives subordonnées.*

III. Soit

$$5. \quad a^\lambda = Np + r,$$

où λ est facteur de $p-1$ (3.), il existe toujours λ valeurs différentes de a qui donnent *le même* reste r. Comme $p-1$ est un nombre pair pour tout nombre premier impair, il est toujours divisible par $\lambda = 2$. Donc il existe *toujours* des *couples* de valeurs de a pour chaque *reste quadratique* r. Si $p-1$ est divisible par $\lambda = 3$, il existe des groupes de 3 valeurs de a pour chaque *reste cubique* r etc.

IV. L'équation (5.) donne

$$a^{\tau\lambda} = a^{p-1}(3) = Np + 1\,(1) = (Np + r)^\tau\,(5) = Np + r^\tau,$$

ou bien

$$6. \quad r^\tau = Np + 1.$$

Cela fait voir que les *restes quadratiques, cubiques* etc. sont toujours des *racines secondaires* et jamais des *racines primitives*, parceque déjà la puissance $\tau < p-1$, divisée par p, donne 1 pour reste.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

V. Toutes les puissances des restes quadratiques, cubiques etc. donnent de nouveau des restes du même genre. Car puisque l'équation (5.) a lieu pour toutes les valeurs 1, 2, 3, ... $p-1$ de α, et que α^2, α^3, α^4, ..., en en retranchant un multiple convenable de p, rentrent toujours dans ces mêmes valeurs, les puissances successives de r rentreront également dans le cadre de ces restes.

VI. Si, comme dans le cas actuel, on cherche non une racine primitive *isolée*, mais *toutes* ces racines en même tems, on pourrait déjà tirer de la remarque (IV.) une méthode assez expéditive pour le calcul de ces racines. Car il ne s'agirait que de calculer les restes quadratiques, les restes cubiques, s'il y en a d'égaux, c'est-à-dire si $p-1$ est divisible par 3, etc., et généralement les restes des puissances dont l'exposant est diviseur de $p-1$. Comme tous ces restes ne peuvent etre des racines primitives, celles-ci se trouveroient sur le champ, en effaçant dans la série 1, 2, 3, 4, ... $p-1$ les restes calculés. Et d'ailleurs le calcul de ces restes serait assez facile, en profitant de la remarque (V.). Car il n'y auroit qu'à prendre les puissances diverses d'un reste quelconque, dont on connaît toujours l'un ou l'autre, par ex. des nombres 4, 9, 16, ... qui sont restes quadratiques; des nombres 8, 27, 64, ... qui sont restes cubiques etc. Ce seroit même une méthode *directe* de calcul, dans le cas où l'on désire en même tems les restes des puissances, dont il s'agit, parcequ'il n'y auroit pas de tâtonnement.

VII. Mais cette méthode a l'inconvénient que les puissances d'un seul reste quadratique, cubique, bien qu'elles ne donnent autre chose que des restes du même genre, n'en donnent pourtant pas *tous* les restes qu'on cherche, puisque déjà $r^\tau = Np + \alpha^{p-1} = Np + 1$, de sorte qu'on ne trouve pas tous les $p-1$ restes, mais seulement τ restes. Pour avoir les autres, il faut calculer de nouveau les puissances de quelques autres restes.

VIII. Par cette raison on a préféré une autre méthode, que l'exemple suivant éclaircira suffisamment. Cet exemple est choisi parmi ceux qui offrent plus de difficultés que les autres, et il suffira de faire voir les règles du calcul.

IX. Soit proposé le nombre premier $p = 41$.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

Voilà le tableau du calcul:

1.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2.	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
3.	2	4	8	16	32	23	5	10	20	40	39	37	33	25	9	18	36	31	21	1
4.	3	6	9	12	15	18	21	24	27	30	33	36	39	1	4	7	10	13	16	19
5.	3	9	27	40	38	32	14	1												
6.	6	12	18	24	30	36	1	7	13	19	25	31	37	2	8	14	20	26	32	38
7.	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40
8.	6		36		11		25		27		39		29		10		19		32	
	35		5		30		16		14		2		12		31		22		9	
9.					6				36					11					25	
					19				32					28					4	
					26				33					34					40	
					14				2					12					31	
					17				20					38					23	

1.	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
2.	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
3.																				
4.	22	25	28	31	34	37	40	2	5	8	11	14	17	20	23	26	29	32	35	38
5.																				
6.	3	9	15	21	27	33	39	4	10	16	22	28	34	40	5	11	17	23	29	35
7.	35	5	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1
8.	28		4		24		21		3		18		26		33		34		40	
	13		37		17		20		38		23		15		8		7		1	
9.					27				39					29					10	
					24				21					3					18	
					35				5					30					16	
					22				9					13					37	
					15				8					7					1	

Voici aussi les règles.

1. Ecrivez sur une première ligne les nombres naturels 1, 2, 3, ... 40.

2. Ecrivez dessous, sur une seconde ligne, les multiples de 2, en ayant attention d'en retrancher $p = 41$, aussitôt que les multiples de 2 surpassent 41. Cela se fait sans un calcul proprement dit.

3. Maintenant les nombres de la seconde ligne vous donneront déjà *sans* nouveau calcul les diverses *puissances* de 2. Car au dessous du nombre 2 de la première ligne vous trouvez dans la seconde ligne $4 = 2^2$; au dessous de 4 de la première ligne vous trouvez dans la seconde ligne $8 = 2^3$, au dessous de 8 vous trouvez $16 = 2^4$, sous 16 vous trouvez

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$32 = 2^5$, sous 32 vous trouvez $23 = 2^6 - Np$ etc. Donc il n'y a qu'à *copier* les nombres de la ligne précèdente et à *écrire* la *troisième* ligne, qui présentera les diverses puissances de 2, ou plutôt les restes que laissent ces puissances, si on les divise par p.

4. Si aucun de ces restes, autre que le *dernier*, étoit $= 1$, le nombre 2 seroit nécessairement une racine primitive. Mais dans le cas actuel on trouve que déjà $2^{20} = Np + 1$. Donc 2 n'est pas une racine primitive.

5. Essayez donc le suivant nombre premier 3. Ecrivez sur une quatrième ligne les multiples de 3, précisément de la même manière que vous avez employée pour le nombre 2 (2.) et puis extrayez de ces multiples les diverses puissances de 3 d'après la même règle suivie en (3.) pour le nombre 2. Ecrivez les sur une cinquième ligne.

6. Vous trouverez que dans le cas actuel 3 n'est pas non plus une racine primitive, parcequ'on a déjà $3^8 = Np + 1$.

7. Maintenant, au lieu d'essayer le nombre premier suivant 5, vous pourrez déjà être sûr que $2.3 = 6$ est effectivement une racine primitive. Car si ce nombre ne l'étoit pas, on ne pourroit avoir que 6^2, ou 6^4, ou 6^5, ou 6^8, ou 6^{10}, ou $6^{20} = Np + 1$; 2, 4, 5, 8, 10, 20 étant les seuls facteurs de $p - 1 = 40$. Mais suivant le calcul déjà fait on a

$$7. \quad \begin{cases} 2^2 = Np + 4, & 2^5 = Np + 32 = Np - 9, \\ 3^2 = Np + 9, & 3^5 = Np + 38 = Np - 3. \end{cases}$$

donc

$$8. \quad (2.3)^2 = 6^2 = Np + 36 = Np - 5, \quad (2.3)^5 = 6^5 = Np + 27 = Np - 14$$

et de là

$$9. \quad \begin{cases} 6^4 = Np + 25 = Np - 16, & 6^{10} = Np + 32 = Np - 9, \\ 6^8 = Np + 10, & 6^{20} = Np + 40. \end{cases}$$

8. Cela étant trouvé, écrivez sur une sixième ligne les multiples de 6 suivant la règle de (2. et 5.), et puis extrayez en les puissances diverses de 6 d'après la règle de (3. et 5.).

9. Ici finit déjà tout le *calcul*, si d'ailleurs on veut nommer *calcul* la simple écriture des multiples d'un nombre peu considérable, comme 2, 3, 6 etc. Dès ici vous trouverez tous les résultats par la simple *copie* de nombres déjà calculés, en les mettant à leurs places, et puis en ordre.

10. En effet, le reste 36 (ligne 7.) de la 2^{me} puissance de 6 étant le *reste quadratique* de ce nombre, celui 25 (ligne 7.) de la 4^{me} puissance

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

de 6 sera également *reste quadratique* de $6^2 = 36$, celui 39 (ligne 7.) de la 6me puissance de 6 sera *reste quadratique* de $6^3 = Np + 11$; 10 sera *reste quadratique* de $6^4 = Np + 25$ etc. Donc il n'y a qu'à *écrire* les nombres de la 7me ligne au dessous *d'eux mêmes*, en laissant toujours alternativement une colonne vide. Etant arrivé de cette manière au dernier reste 1, auquel répond le nombre 40, on continue en commençant derechef. Les nombres 6,35; 36,5, 11,30...., placés de cette sorte au-dessous de ceux de la 7me ligne, seront ceux (8.), dont les nombres de la 7me ligne, qui se trouvent au-dessus, sont les *restes quadratiques.*

On voit par les mêmes raisons que si l'on écrit les nombres de la 7me ligne également au-dessous deux mêmes, mais en laissant toujours 4 colonnes vides, comme dans (9.), ces nombres (9.) seront ceux dont les nombres 27, 32, 3 etc. de la 7me ligne qui se trouvent au-dessus, sont *les restes de leurs* 5mes *puissances.* Et ainsi de toutes les autres puissances.

12. Mais $p - 1 = 40$ n'ayant pas d'autres diviseurs premiers que 2 et 5, tous les nombres de la 7me ligne qui ne sont ni restes quadratiques ni restes de puissances cinquièmes, seront nécessairement des *racines primitives.* Donc les nombres 6, 11, 29, 19, 28 etc., au-dessous desquels ou ne rencontre ni racines 2mes ni racines 5mes, sont les *racines primitives cherchées.*

13. Vous avez trouvé jusqu'ici les restes des 2mes et 5mes etc. puissances de nombres 1, 2, 3.... $p-1$, avec les racines qui correspondent à un même *reste*, et de plus les racines primitives du nombre premier donné. Pour trouver encore les racines *secondaires*, il faut premièrement *mettre en ordre* les résultats trouvés jusqu'ici. Cela ce fait comme suit.

14. Copiez les restes quadratiques 36, 25, 39 etc. dans l'ordre où ils sont, mais en les plaçant en colonnes par dixaines, de la manière suivante:

8.

4	10	25	36	40
5	18	21	39	
2	16	20	32	
9		23	33	
8			31	
1			37	

D'après ce petit tableau vous pourrez les ranger dans leur ordre naturel par le seul coup d'oeil, et cela vous donnera la première ligne $r = 1, 2, 4, 5, \ldots$ de la table à construire (voy. $p = 41$ dans cette table plus bas).

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

Cela fait, mettez les racines 6,35 (ligne 8 tableau de calcul IX.) au-dessous du reste quadratique 36 (table page 44, $p = 41$), les racines 36,5 au-dessous du reste quadratique 25, les racines 11,30 au-dessous du reste quadratique 39 etc. Cela vous donnera les valeurs de a de la table pour $a^2 = Np + r$.

15. Faites précisément les mêmes opérations avec les restes des 5^{mes} puissances du tableau (IX.) et avec leurs racines, et vous aurez les valeurs de r et a dans $a^5 = Np + r$ pour la table à construire etc.

16. Dès ici vous n'avez plus besoin du tableau (IX.), mais vous pourrez tirer de la table commencée elle même, les resultats dont il s'agit encore.

Supposez pour cela x successivement égal à tout les facteurs de $p - 1 = 40$, savoir $x = 40, 20, 10, 8, 5, 4, 2, 1$.

17. Commencez par le plus petit facteur 1. Il est clair que si $a^x = Np + 1$, il n'y a d'autre valeur de a que 1, car la première puissance d'aucun autre nombre que 1, divisée par p, ne laisse 1 pour reste.

18. Maintenant la partie de la table qui se rapporte à l'équation $a^2 = Np + r$ fait voir, que pour $r = 1$ il n'y a d'autre valeur de a que 1 et 40. Donc si l'on veut que dans $a^x = Np + 1$, x soit $= 2$, a ne peut être que 1 ou 40, et 1 ayant été déjà réservé pour $x = 1$, on a $a = 40$ pour $x = 2$.

19. Vient $x = 4$. Cherchez la valeur 40 de a pour $x = 2$ parmi les valeurs de r dans $a^2 = Np + r$: vous trouverez qu'il n'y a que les deux nombres 9 et 32 dont la 2^{me} puissance, divisée par p, laisse 40 pour reste, et 40^2 étant $= Np + 1$, on voit que la 4^{me} puissance de 9 et 32 donne $Np + 1$, et que cela n'a lieu pour aucune puissance moins élevée. Donc si l'on veut que dans $a^x = Np + 1$, x soit $= 4$, il n'y a d'autres valeurs de a que 9 et 32.

20. Pour avoir a dans $a^5 = Np + 1$, il n'y a qu'à chercher la valeur 1 de r dans $a^5 = Np + r$. Ou trouve que, 1 excepté, il n'y a d'autres valeurs de a pour $a^5 = Np + 1$ que 10, 16, 18, 37.

20. Soit $x = 8$ dans $a^x = Np + 1$. Il n'y a qu'à chercher les valeurs 9 et 32 de a dans $a^4 = Np + 1$ parmi celles de r dans $a^2 = Np + r$. Cela fait voir que 3^2, $38^2 = Np + 9$ et 14^2, $27^2 = Np + 32$. Donc 3^8, $8^8 = (Np + 9)^4 = Np + 1$ et 14^8, $22^8 = (Np + 32)^4 = Np + 1$. Donc les valeurs de a pour $a^8 = Np + 1$ sont 3, 14, 27, 38, et il n'y en a pas d'autres.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

21. Pour trouver les valeurs de a pour $a^{10} = Np + 1$, on cherchera la valeur 40 de a pour $a^2 = Np + 1$ parmi les restes r de $a^5 = Np + r$. On trouve que les nombres 4, 23, 25, 31, 40 conviennent à ce reste, et en effaçant celui 40, qui est déjà réservé à $x = 2$, on voit qu'il n'y a pas d'autres valeurs de a pour $a^{10} = Np + 1$ que 4, 23, 25, 31.

22. Pour trouver les valeurs de a pour $a^{20} = Np + 1$, on cherchera les valeurs 9 et 32 de a pour $a^4 = Np + 1$ parmi les restes r de $a^5 = Np + r$. On trouve que les nombres 5, 8, 9, 21, 39, 2, 20, 32, 33 et 36 conviennent à ces restes, et en supprimant les nombres 9 et 32, déjà employés, on a 2, 5, 8, 20, 21, 33, 36, 39 pour les valeurs de a dans $a^{20} = Np + 1$.

23. Enfin on pourroit trouver les valeurs de a pour $a^{40} = Np + 1$, c'est-à-dire les *racines primitives* elles mêmes, par le même procédé, savoir, en cherchant les valeurs de a pour $a^{20} = Np + 1$ parmi celles des r dans $a^2 = Np + r$ ou les valeurs de a pour $a^8 = Np + 1$ parmi celles de r dans $a^5 = Np + r$. Mais les racines primitives ayant été déjà mises en évidence dans le tableau de calcul (IX.), comme il a été remarqué (12.), il n'y a qu'à les copier.

24. Voilà achevée la table pour le nombre premier donné 41. On procèdera de la même manière pour tout autre nombre premier.

Nous dirons encore deux mots sur la certitude et la facilité du calcul employé.

25. La certitude en est favorisée premièrement par la simplicité extrême des procédés, qui pour la plupart se réduisent à *copier* des nombres. Et plus un calcul s'éxécute pour ainsi dire *mécaniquement*, plus il est sûr et à l'abri des erreurs.

En second lieu les résultats du calcul sont garantis continuellement par des *preuves* nombreuses. Par exemple: les sommes des nombres dont les 2^{me} les 5^{me} puissances etc. divisées par p donnent *le même* reste, sont toujours divisible par p.

Les restes des puissances, multipliés par l'un quelconque d'entre eux, doivent toujours se reproduire eux mêmes.

Les racines primitives et les racines secondaires, prises ensemble, doivent toujours parcourir tous les nombres $1, 2, 3 \ldots\ldots p-1$ sans toucher à aucun plus d'une fois.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

Les racines primitives et les racines secondaires doivent toujours se presenter en nombre *pair*, et leur nombre doit être égal à celui des nombres qui n'ont pas de diviseur commun avec l'exposant, et qu'on trouve facilement par une formule connue.

Les racines primitives sont toujours des nombres *correspondants*, c'est-à-dire, que leurs produits, pris par couples, doivent être $= Np+1$; etc.

Toutes ces conditions peuvent servir de preuves du calcul, et leur application s'offre comme d'elle même dans son cours.

26. La *facilité* du calcul vient également de sa simplicité. L'exemple que nous avons choisi pour servir d'éclaircissement, est plus embarrassant que les autres, parceque deux essais, sans effêt, étoient nécessaires pour trouver une première racine primitive. Souvent 2, ou au moins 3, est une racine primitive, donc alors le premier, ou au moins le second essai réussit déjà, et l'opération se simplifie encore considérablement. La facilité du calcul est telle, que pour faire la première partie du calcul décrit ci-dessus (1 jusque 12 inclusivement) pour les 25 nombres premiers 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 et 101, il n'a fallu que 8 heures de tems, et environ autant pour l'extraction des résultats et pour l'arrangement de la table.

Il seroit peut être à désirer que quelqu'un qui aurait le loisir et l'envie de continuer encore plus loin cette table, le fît. C'est surtout par cette raison que j'espère qu'on me pardonnera le detail minutieux dans lequel je me suis permis d'entrer, en faisant le rapport du calcul employé.

Additions.

I. La table décrite ci-dessus, pour être complète, devoit non seulement présenter les restes des puissances dont l'exposant est diviseur de $p-1$, mais encore les restes de *toutes* les autres puissances depuis la première jusqu'à la $p-1^{\text{me}}$. Pour donner un exemple d'un telle table *complète*, j'ai calculé encore ces autres restes pour les nombres premiers depuis 3 jusqu'à 29, où je me suis arrêté, pour ne pas trop grossir la table. Le reste de la table, pour les nombres premiers depuis 31 jusqu'à 101, est resté tel qu'il étoit originairement. Je laisse à qui le voudra le soin de continuer le calcul supplémentaire, qui d'ailleurs n'a pas la moindre difficulté, puisqu'il n'y à qu'à écrire les restes des diverses puissances d'une

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

racine primitive quelconque au-dessous d'eux mêmes, en laissant successivement 1, 2, 3, 4..... colonnes alternativement vides.

II. Pour servir d'exemple au problème: *de trouver les divers nombres premiers dont un nombre donné est racine primitive*, j'ai extrait de la table ci-dessus un tableau des racines primitives des divers nombres premiers depuis 3 jusqu'à 101, qu'on trouve à la suite de la table ci-jointe. Ce tableau fait voir par ex.:

que 2 est racine primitive de 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101,
que 3 est racine primitive de 5, 7, 17, 19, 29, 31, 43, 53, 79, 89, 101,
etc.

Table

des restes que laissent les puissances des nombres naturels, si on les divise par les nombres premiers depuis 3 jusqu'à 101, et des racines primitives et secondaires pour les mêmes nombres premiers.

$$\boxed{p = 3}$$

$$a^2 = Np + r$$

$$r = 1$$

$$a = 1, 2$$

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 2$, $a = 2$ (rac. pr.)
$x = 1$, $a = 1$

$$\boxed{p = 5}$$

$$a_n^n = Np + r$$

$$r = 1, 2, 3, 4$$

$$a_3 = 1 \quad 3 \quad 2 \quad 4$$

$$r = 1, 4$$

$$a_2 = 1, 4 \quad 2, 3$$

$$a^{\alpha\,(\text{min.})} = Np + 1$$

$\alpha = 4$, $a = 2, 3$ (rac. pr.)
$\alpha = 2$, $a = 4$
$\alpha = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$$\boxed{p = 7}$$

$$a_n^n = Np + r$$

$$r = 1, 2, 3, 4, 5, 6$$

$a_5 =$ 1 4 5 2 3 6

$$r = 1, \quad 2, \quad 4$$

$a_2 =$ 1, 6 3, 4 2, 5

$a_4 =$ 1, 6 2, 4 3, 5

$$r = 1, \quad 6$$

$a_3 =$ 1, 2, 4 3, 5, 6

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 6,\ a = 3, 5$ (rac. pr.)
$x = 3,\ a = 2, 4$
$x = 2,\ a = 6$
$x = 1,\ a = 1$

$$\boxed{p = 11}$$

$$a_n^n = Np + r$$

$$r = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

$a_3 =$ 1 7 9 5 3 8 6 2 4 10

$a_7 =$ 1 8 5 9 4 7 2 6 3 10

$a_9 =$ 1 6 4 3 9 2 8 7 5 10

$$r = 1, \quad 3, \quad 4, \quad 5, \quad 9$$

$a_2 =$ 1, 10 5, 6 2, 9 4, 7 3, 8

$a_4 =$ 1, 10 4, 7 3, 8 2, 9 5, 6

$a_6 =$ 1, 10 3, 8 4, 7 5, 6 2, 9

$a_8 =$ 1, 10 2, 9 5, 6 3, 8 4, 7

$$r = 1, \qquad 10$$

$a_5 =$ 1, 3, 4, 5, 9 2, 6, 7, 8, 10

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 10,\ a = 2, 6, 7, 8$ (rac. pr.)
$x = 5,\ a = 3, 4, 5, 9$
$x = 2,\ a = 10$
$x = 1,\ a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 13$

$$a_n^r = Np + r$$

$r =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12
$a_5 =$	1	6	9	10	5	2	11	8	3	4	7	12
$a_7 =$	1	11	3	4	8	7	6	5	9	10	2	12
$a_{11} =$	1	7	9	10	8	11	2	5	3	4	6	12

$r =$	1,	3,	4,	9,	10,	12,
$a_2 =$	1, 12	4, 9	2, 11	3, 10	6, 7	5, 8
$a_{10} =$	1, 12	3, 10	6, 7	4, 9	2, 11	5, 8

$r =$	1,	5,	8,	12,
$a_3 =$	1, 3, 9	7, 8, 11	2, 5, 6	4, 10, 12
$a_9 =$	1, 3, 9	2, 5, 6	7, 8, 11	4, 10, 12

$r =$	1,	3,	9
$a_4 =$	1, 5, 8, 12	2, 3, 10, 11	4, 6, 7, 9
$a_8 =$	1, 5, 8, 12	4, 6, 7, 9	2, 3, 10, 11

$r =$	1,	12	
$a_6 =$	1, 3, 4, 9, 10, 12	2, 5, 6, 7, 8, 11	

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 12$, $a = 2, 6, 7, 11$ (rac. pr.)
$x = 6$, $a = 4, 10$
$x = 4$, $a = 5, 8$
$x = 3$, $a = 3, 9$
$x = 2$, $a = 12$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 17$

$$a_n^n = Np + r$$

$r =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16
$a_3 =$	1	8	7	13	11	5	14	2	15	3	12	6	4	10	9	16
$a_5 =$	1	15	12	4	3	10	6	9	8	11	7	14	13	5	2	16
$a_7 =$	1	9	11	13	10	14	12	15	2	5	3	7	4	6	8	16
$a_9 =$	1	2	14	4	12	11	10	8	9	7	6	5	13	3	15	16
$a_{11} =$	1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16
$a_{13} =$	1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16
$a_{15} =$	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16

$r =$	1,	2,	4,	8,	9,	13,	15,	16
$a_2 =$	1, 16	6, 11	2, 15	5, 12	3, 14	8, 9	7, 10	4, 13
$a_6 =$	1, 16	5, 12	8, 9	6, 11	7, 10	2, 15	3, 14	4, 13
$a_{10} =$	1, 16	7, 10	2, 15	3, 14	5, 12	8, 9	6, 11	4, 13
$a_{14} =$	1, 16	3, 14	8, 9	7, 10	6, 11	2, 15	5, 12	4, 13

$r =$	1,	4,	13,	16
$a_4 =$	1, 4, 13, 16	6, 7, 10, 11	3, 5, 12, 14	2, 8, 9, 15
$a_{12} =$	1, 4, 13, 16	3, 5, 12, 14	6, 7, 10, 11	2, 8, 9, 15

$r =$	1,	16
$a_8 =$	1, 2, 4, 8, 9, 13, 15, 16	3, 5, 6, 7, 10, 11, 12, 14

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 16$, $a = 3, 5, 6, 7, 10\ 11, 12, 14$ **(rac. pr.)**
$x = 8$, $a = 2, 8, 9, 15$
$x = 4$, $a = 4, 13$
$x = 2$, $a = 16$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 19$

$$a_n^n = Np + r$$

$r =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18
$a_5 =$	1	15	10	16	6	17	11	12	5	14	7	8	2	13	3	9	4	18
$a_7 =$	1	3	14	9	17	4	7	8	6	13	11	12	15	2	10	5	16	18
$a_{11} =$	1	13	15	17	9	5	11	12	16	3	7	8	14	10	2	4	6	18
$a_{13} =$	1	14	2	6	16	9	7	8	4	15	11	12	10	3	13	17	5	18
$a_{17} =$	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18

$r =$	1,	4,	5,	6,	7,	9,	11,	16,	17
$a_2 =$	1, 18	2, 17	9, 10	5, 14	8, 11	3, 16	7, 12	4, 15	6, 13
$a_4 =$	1, 18	6, 13	3, 16	9, 10	7, 12	4, 15	8, 11	2, 17	5, 14
$a_8 =$	1, 18	5, 14	4, 15	3, 16	8, 11	2, 17	7, 12	6, 13	9, 10
$a_{10} =$	1, 18	4, 15	5, 14	6, 13	7, 12	9, 10	8, 11	3, 16	2, 17
$a_{14} =$	1, 18	3, 16	6, 13	2, 17	8, 11	5, 14	7, 12	9, 10	4, 15
$a_{16} =$	1, 18	9, 10	2, 17	4, 15	7, 12	6, 13	8, 11	5, 14	3, 16

$r =$	1,	7,	8,	11,	12,	18
$a_3 =$	1, 7, 11	4, 6, 9	2, 3, 14	5, 16, 17	10, 13, 15	8, 12, 18
$a_{15} =$	1, 7, 11	5, 16, 17	10, 13, 15	4, 6, 9	2, 3, 14	8, 12, 18

$r =$	1,	7,	11
$a_6 =$	1, 7, 8, 11, 12, 18	2, 3, 5, 14, 16, 17	4, 6, 9, 10, 13, 15
$a_{12} =$	1, 7, 8, 11, 12, 18	4, 6, 9, 10, 13, 15	2, 3, 5, 14, 16 17

$r =$	1,	18
$a_9 =$	2, 3, 8, 10, 12, 13, 14, 15, 18	1, 4, 5, 6, 7, 9, 11, 16, 17

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 18$, $a = 2, 3, 10, 13, 14, 15$ (rac. pr.)
$x = 9$, $a = 4, 5, 6, 9, 16, 17$
$x = 6$, $a = 8, 12$
$x = 3$, $a = 7, 11$
$x = 2$, $a = 18$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 23$

$$a_n^n = Np + r$$

$r =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$a_3 =$	1	16	12	3	19	8	14	2	6	5	10	13	18	17	21	9	15	4	20	11	7	22
$a_5 =$	1	6	18	13	11	16	15	9	2	20	19	4	13	21	14	8	7	12	10	5	17	22
$a_7 =$	1	3	6	9	7	18	11	4	13	21	15	8	2	10	19	12	5	16	14	17	20	22
$a_9 =$	1	9	13	12	20	2	17	16	8	19	5	18	4	15	7	6	21	3	11	10	14	22
$a_{13} =$	1	18	16	2	15	12	19	13	3	17	14	9	6	20	10	4	11	8	21	7	5	22
$a_{15} =$	1	8	4	18	10	9	21	6	16	11	20	3	12	7	17	2	14	13	5	19	15	22
$a_{17} =$	1	4	9	16	21	13	20	18	12	15	17	6	8	11	5	3	10	2	7	14	19	22
$a_{19} =$	1	13	2	8	17	3	5	12	4	14	7	16	9	19	11	18	20	6	15	21	10	22
$a_{21} =$	1	12	8	6	14	4	10	3	18	7	21	2	16	5	20	13	19	9	17	15	11	22

$r =$	1,	2,	3,	4,	6,	8,	9,	12,	13,	16,	18
$a_2 =$	1, 22	5, 18	7, 16	2, 21	11, 12	10, 13	3, 20	9, 14	6, 17	4, 19	8, 15
$a_4 =$	1, 22	8, 15	4, 19	5, 18	9, 14	6, 17	7, 16	3, 20	11, 12	2, 21	10, 13
$a_6 =$	1, 22	4, 19	9, 14	7, 16	10, 13	5, 18	11, 12	6, 17	8, 15	3, 20	2, 21
$a_8 =$	1, 22	10, 13	2, 21	8, 15	3, 20	11, 12	4, 19	7, 16	9, 14	5, 18	6, 17
$a_{10} =$	1, 22	11, 12	8, 15	6, 17	4, 19	3, 20	5, 18	2, 21	7, 16	10, 13	9, 14
$a_{12} =$	1, 22	2, 21	3, 20	4, 19	6, 17	8, 15	9, 14	11, 12	10, 13	7, 16	5, 18
$a_{14} =$	1, 22	4, 19	11, 12	3, 20	8, 15	2, 21	6, 17	10, 13	5, 18	9, 14	4, 19
$a_{16} =$	1, 22	6, 17	5, 18	10, 13	7, 16	9, 14	2, 21	4, 19	3, 20	8, 15	11, 12
$a_{18} =$	1, 22	3, 20	6, 17	9, 14	5, 18	4, 19	10, 13	8, 15	2, 21	11, 12	7, 16
$a_{20} =$	1, 22	9, 14	10, 13	11, 12	2, 21	7, 16	8, 15	5, 18	4, 19	6, 17	3, 20

$r =$	1,	22,
$a_{11} =$	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18	5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 22$, $a = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$ (rac. pr.)
$x = 11$, $a = 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$
$x = 2$, $a = 22$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 29$

$$a_n^n = Np + r$$

$r =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$a_3 =$	1	26	18	9	22	4	16	2	5	21	15	17	6	10	19	23	12	14	8	24	27	13	25	7	20	11	3	28
$a_5 =$	1	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14	25	19	5	16	20	23	27	8	28
$a_9 =$	1	11	14	5	13	9	23	26	22	27	19	12	4	21	8	25	17	10	2	7	3	6	20	16	24	15	18	28
$a_{11} =$	1	10	8	13	4	22	20	14	6	11	27	17	5	26	3	24	12	2	18	23	15	9	7	25	16	21	19	28
$a_{13} =$	1	14	19	22	6	5	25	18	13	26	21	12	9	2	27	20	17	8	3	16	11	4	24	23	7	10	15	28
$a_{15} =$	1	27	26	4	5	6	7	21	9	19	18	17	13	15	14	16	12	11	10	20	8	22	23	24	25	3	2	28
$a_{17} =$	1	3	11	9	22	4	16	27	5	8	14	12	6	19	10	23	17	15	21	24	2	13	25	7	20	18	26	28
$a_{19} =$	1	8	27	6	9	13	24	19	4	14	26	17	22	18	11	7	12	3	15	25	10	5	16	20	23	2	21	28
$a_{23} =$	1	18	15	5	13	9	23	3	22	2	10	17	4	8	21	25	12	19	27	7	26	6	20	16	24	14	11	28
$a_{25} =$	1	19	21	13	4	22	20	15	6	18	2	12	5	3	26	24	17	27	11	23	14	9	7	25	16	8	10	28
$a_{27} =$	1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

$r =$	1,	4,	5,	6,	7,	9,	13,	16,	20,	22,	23,	24,	25,	28
$a_2 =$	1, 28	2, 27	11, 18	8, 21	6, 23	3, 26	10, 19	4, 25	7, 22	14, 55	9, 20	13, 16	5, 24	12, 17
$a_6 =$	1, 28	3, 26	14, 15	2, 27	4, 25	11, 18	8, 21	9, 20	13, 16	10, 19	5, 24	6, 23	7, 22	12, 17
$a_{10} =$	1, 28	8, 21	3, 26	10, 19	13, 16	2, 27	14, 15	6, 23	5, 24	11, 18	4, 25	7, 22	9, 20	12, 17
$a_{18} =$	1, 28	11, 18	10, 19	3, 26	9, 20	14, 15	2, 27	5, 24	6, 23	8, 21	7, 22	4, 25	13, 16	12, 17
$a_{22} =$	1, 28	10, 19	2, 27	14, 15	7, 22	8, 21	11, 18	13, 16	9, 20	3, 26	6, 23	5, 24	4, 25	12, 17
$a_{26} =$	1, 28	14, 15	8, 21	11, 18	5, 24	10, 19	3, 26	7, 22	4, 25	2, 27	13, 16	9, 20	6, 23	12, 17

$r =$	1,	7,	16,	20,	23,	24
$a_4 =$	1, 12, 17, 28	8, 9, 20, 21	2, 5, 24, 27	6, 14, 15, 23	3, 7, 22, 26	4, 10, 19, 25
$a_8 =$	1, 12, 17, 28	3, 7, 22, 26	11, 13, 16, 18	8, 9, 20, 21	6, 14, 15, 23	2, 5, 24, 27
$a_{12} =$	1, 12, 17, 28	2, 5, 24, 27	3, 7, 22, 26	4, 10, 19, 25	11, 13, 16, 18	8, 9, 20, 21
$a_{16} =$	1, 12, 17, 28	6, 14, 15, 23	4, 10, 19, 25	3, 7, 22, 26	8, 9, 20, 21	11, 13, 16, 18
$a_{20} =$	1, 12, 17, 28	4, 10, 19, 25	8, 9, 20, 21	11, 13, 16, 18	2, 5, 24, 27	6, 14, 15, 23
$a_{24} =$	1, 12, 17, 28	11, 13, 16, 18	6, 14, 15, 23	2, 5, 24, 27	5, 10, 19, 25	3, 7, 22, 26

$r =$	1,	12,	17,	28
$a_7 =$	1, 7, 16, 20, 23, 24, 25	2, 3, 11, 14, 17, 19, 21	8, 10, 12, 15, 18, 26, 27	4, 5, 6, 9, 13, 22, 28
$a_{21} =$	1, 7, 16, 20, 23, 24, 25	8, 10, 12, 15, 18, 26, 27	2, 3, 11, 14, 17, 19, 21	4, 5, 6, 9, 13, 22, 28

$r =$	1,	28
$a_{14} =$	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27

$$a^{x(\min.)} = Np + 1$$

$x = 28$, $a = 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27$ (rac. pr.)
$x = 14$, $a = 4, 5, 6, 9, 13, 22$
$x = 7$, $a = 7, 16, 20, 23, 24, 25$
$x = 4$, $a = 12, 17$
$x = 2$, $a = 28$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 31$

$$a^2 = Np + r$$

$r =$	1,	2,	4,	5,	7,	8,	9,	10,	14,	16,	18,	19	20,	25	28
$a =$	1, 30	8, 23	2, 29	6, 25	10, 21	15, 16	3, 28	14, 17	13, 18	4, 27	7, 24	9, 22	12, 19	5, 26	11, 20

$$a^3 = Np + r$$

$r =$	1,	2,	4,	8,	15,	16,	23,	27,	29,	30
$a =$	1, 5, 25	4, 7, 20	16, 18, 28	2, 10, 19	17, 22, 23	8, 9, 14	12, 21, 29	3, 13, 15	11, 24, 27	6, 26, 30

$$a^5 = Np + r$$

$r =$	1,	5,	6,	25,	26,	30
$a =$	1, 2, 4, 8, 16	7, 14, 19, 25, 28	11, 13, 21, 22, 26	5, 9, 10, 18, 20	3, 6, 12, 17, 24	15, 23, 27, 29, 30

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 30$, $a = 3, 11, 12, 13, 17, 21, 22, 24$ (rac. pr.)
$x = 15$, $a = 7, 9, 10, 14, 18, 19, 20, 28$
$x = 10$, $a = 15, 23, 27, 29$
$x = 6$, $a = 6, 26$
$x = 5$, $a = 2, 4, 8, 16$
$x = 3$, $a = 5, 25$
$x = 2$, $a = 30$
$x = 1$, $a = 1$

$p = 37$

$$a^2 = Np + r$$

$r =$	1,	3,	4,	7,	9,	10,	11,	12,	16,	21,	25,	26,	27,	28,	30,	33,	34,	36
$a =$	1	15	2	9	3	11	14	7	4	13	5	10	8	18	17	12	16	6
	36	22	35	28	34	26	23	30	33	24	32	27	29	19	20	25	21	31

$$a^3 = Np + r$$

$r =$	1,	6,	8,	10,	11,	14,	23,	26,	27,	29,	31,	36
$a =$	1, 10, 26	14, 29, 31	2, 15, 20	7, 33, 34	21, 25, 28	5, 13, 19	18, 24, 32	9, 12, 16	3, 4, 30	17, 22, 35	6, 8, 23	11, 27, 36

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 36$, $a = 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35$ (rac. pr.)
$x = 18$, $a = 3, 4, 21, 25, 28, 30$
$x = 12$, $a = 8, 14, 23, 29$
$x = 9$, $a = 7, 9, 12, 16, 33, 34$
$x = 6$, $a = 11, 27$
$x = 4$, $a = 6, 31$
$x = 3$, $a = 10, 26$
$x = 2$, $a = 36$
$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 41$

$$a^2 = Np + r$$

$r =$ 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40

$a =$ {1 17 2 13 7 3 16 4 10 15 12 8 5 20 14 19 6 18 11 9 / 40 24 39 28 34 38 25 37 31 26 29 33 36 21 27 22 35 23 30 32}

$$a^5 = Np + r$$

$r =$	1,	3,	9,	14,	27,	32,	38,	40
$a =$	1, 10, 16 / 18, 37	11, 12, 28 / 34, 38	5, 8, 9 / 21, 39	15, 22, 24 / 27, 35	6, 14, 17 / 19, 26	2, 20, 32 / 33, 36	3, 7, 13 / 29, 30	4, 23, 25 / 31, 40

$$a^{x\,(\min.)} = Np + 1$$

$x = 40$, $a =$ 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35 (rac. pr.)
$x = 20$, $a =$ 2, 5, 8, 20, 21, 33, 36, 39
$x = 10$, $a =$ 4, 23, 25, 31
$x =$ 8, $a =$ 3, 14, 27, 38
$x =$ 5, $a =$ 10, 16, 18, 37
$x =$ 4, $a =$ 9, 32
$x =$ 2, $a =$ 40
$x =$ 1, $a =$ 1

$p = 43$

$$a^2 = Np + r$$

$r =$ 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41

$a =$ {1 2 7 3 15 21 20 10 12 4 19 8 18 14 5 17 11 6 9 13 16 / 42 41 36 40 28 22 23 33 31 39 24 35 25 29 38 26 32 37 34 30 27}

$$a^3 = Np + r$$

$r =$	1,	2,	4,	8,	11,	16,	21,	22,	27,	32,	35,	39,	41,	42,
$a =$	1, 6 / 41	20, 32 / 34	13, 35 / 38	2, 12 / 29	10, 16 / 17	21, 25 / 40	4, 15 / 24	19, 28 / 39	3, 18 / 22	26, 27 / 33	14, 31 / 41	5, 8 / 30	9, 11 / 23	7, 37 / 42

$$a^7 = Np + r$$

$r =$	1	6	7	36	37	42
$a =$	1, 4, 11, 16 / 21, 35, 41	6, 10, 23, 24 / 31, 38, 40	7, 18, 26, 28 / 29, 30, 34	9, 13, 14, 15 / 17, 25, 36	3, 5, 12 19 / 20, 33, 37	2, 8, 22, 27 / 32, 39, 42

$$a^{x\,(\min.)} = Np + 1$$

$x = 42$, $a =$ 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34 (rac. pr.)
$x = 21$, $a =$ 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40
$x = 14$, $a =$ 2, 8, 22, 27, 32, 39
$x =$ 7, $a =$ 4, 11, 16, 21, 35, 41
$x =$ 6, $a =$ 7, 37
$x =$ 3, $a =$ 6, 36
$x =$ 2, $a =$ 42
$x =$ 1, $a =$ 1

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 47$

$$a^2 = Np + r$$

$r = 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42$

$a =$

1	7	12	2	10	17	14	3	23	22	4	8	21	16	20	5	11	13	19	9	6	15	18
46	40	35	45	37	30	33	44	24	25	43	39	26	31	27	42	36	34	28	38	41	32	29

$$a^{23} = Np + r$$

$r =$	1	46
$a =$	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 46$, $a = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45$ **(rac. pr.)**

$x = 23$, $a = 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42$

$x = 2$, $a = 46$

$x = 1$, $a = 1$

$p = 53$

$$a^2 = Np + r$$

$r = 1,4,6,7,9,10,11,13,15,16,17,24,25,28,29,36,37,38,40,42,43,44,46,47,49,52$

$a =$

1	2	18	22	3	13	8	15	11	4	21	17	5	9	20	6	14	12	26	25	19	16	24	10	7	23
52	51	35	31	50	40	45	38	42	49	32	36	48	44	33	47	39	41	27	28	34	37	29	43	46	30

$$a^{13} = Np + r$$

$r =$	1,	23,	30,	52
$a =$	1, 10, 13, 15, 16, 24, 28 36, 42, 44, 46, 47, 49	5, 8, 12, 14, 18, 21, 22 23, 27, 33, 34, 50, 51	2, 3, 19, 20, 26, 30, 31 32, 35, 39, 41, 45 48	4, 6, 7, 9, 11, 17, 25 29, 37, 38, 40, 43, 52

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 52$, $a = 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51$ **(rac. pr.)**

$x = 26$, $a = 4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43$

$x = 13$, $a = 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49$

$x = 4$, $a = 23, 30$

$x = 2$, $a = 52$

$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 59$

$$a^2 = Np + r$$

$r =$	1,	3,	4,	5,	7,	9,	12,	15,	16,	17,	19,	20,	21,	22,	25,
$a =$	1	11	2	8	19	3	22	29	4	28	14	16	27	9	5
	58	48	57	51	40	56	37	30	55	31	45	43	32	50	54

$r =$	26,	27,	28,	29,	35,	36,	41,	45,	46,	48,	49,	51,	53,	57
$a =$	12	26	21	18	25	6	10	24	20	15	7	13	17	23
	47	33	38	41	34	53	49	35	39	44	52	46	42	36

$$a^{29} = Np + r$$

$r =$	1	58
$a =$	1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56, 58

$$a^{x\,(\min.)} = Np + 1$$

$x = 58$, $a =$ 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56 **(rac. pr.)**

$x = 29$, $a =$ 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57

$x = 2$, $a = 58$

$x = 1$, $a = 1$

$p = 61$

$$a^2 = Np + r$$

$r =$	1,	3,	4,	5,	9,	12,	13,	14,	15,	16,	19,	20,	22,	25,	27
$a =$	1	8	2	26	3	16	14	21	25	4	18	9	12	5	24
	60	53	59	35	58	45	47	40	36	57	43	52	49	56	37

$r =$	34,	36,	39,	41,	42,	45,	46,	47,	48,	49,	52,	56,	57,	58,	60
$a =$	20	6	10	23	15	17	30	13	29	7	28	19	22	27	11
	41	55	51	38	46	44	31	48	32	54	33	42	39	34	50

$$a^3 = Np + r$$

$r =$	1,	3,	8,	9,	11,	20,	23,	24,	27,	28
$a =$	1, 13, 47	4, 5, 52	2, 26, 33	16, 20, 25	32, 40, 60	12, 15, 34	31, 37, 54	8, 10, 43,	3, 19, 39	23, 44, 55

$r =$	33,	34,	37,	38,	41,	50,	52,	53,	58,	60,
$a =$	6, 17, 38	22, 42, 58	18, 51, 53	7, 24, 30	27, 46, 49	11, 21, 29	36, 41, 45	28, 35, 50	9, 56, 57	14, 48, 60

$$a^5 = Np + r$$

$r =$	1,	11,	13,	14,	21,	29,	32,	40,	47,	48,	50,	60
$a =$	1, 9, 20	8, 11, 28	12, 25, 42	5, 39, 45	10, 17, 29	6, 21, 43	5, 7, 18	24, 26, 30	13, 15, 16	4, 14, 19	23, 24, 33	3, 27, 41
	34, 58	37, 38	47, 57	46, 48	31, 35	54, 59	40, 55	32, 51	22, 56	36, 49	50, 53	52, 60

$$a^{x\,(\min.)} = Np + 1$$

$x = 60$, $a =$ 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59 **(rac. pr.)**

$x = 30$, $a =$ 4, 5, 19, 36, 39, 45, 46, 49

$x = 20$, $a =$ 8, 23, 24, 28, 33, 37, 38, 53

$x = 15$, $a =$ 12, 15, 16, 22, 25, 42, 56, 57

$x = 12$, $a =$ 21, 29, 32, 40

$x = 10$, $a =$ 3, 27, 41, 52

$x = 6$, $a =$ 14, 48

$x = 5$, $a =$ 9, 20, 34, 58

$x = 4$, $a =$ 11, 50

$x = 3$, $a =$ 13, 47

$x = 2$, $a = 60$

$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 67$

$$a^2 = Np + r$$

$r =$	1	4	6	9	10	14	15	16	17	19	21	22	23	24	25	26
$a =$	1	2	26	3	12	9	22	4	33	32	17	25	31	15	5	10
	66	65	41	64	55	58	45	63	34	35	50	42	36	52	62	48
$r =$	29	33	35	36	37	39	40	47	49	54	55	56	59	60	62	64	65
$a =$	30	10	13	6	29	21	24	28	7	11	16	18	27	23	14	8	20
	37	57	54	61	38	46	43	39	60	56	51	49	40	44	53	59	47

$$a^3 = Np + r$$

$r =$	1,	3,	5,	8,	9,	14,	15,	22,	24,	25,	27
$a =$	1, 29	18, 53	32, 45	2, 7	16, 56	25, 54	6, 21	24, 26	36, 39	15, 19	3, 20
	37	63	57	58	62	55	40	42	59	33	44
$r =$	40,	42,	43,	45,	52,	53,	58,	59,	62,	64,	66
$a =$	23, 47	34, 48	8, 28	41, 43	27, 46	12, 13	5, 11	9, 60	10, 22	4, 14	30, 3
	64	52	31	50	61	42	51	65	35	49	66

$$a^{11} = Np + r$$

$r =$	1,	29,	30,	37,	38,	66,
$a =$	1, 9, 14, 15, 22, 24	6, 10, 16, 17, 19, 23	7, 11, 12, 20, 31, 32	4, 21, 26, 29, 33, 35	2, 13, 18, 28, 30, 44	3, 5, 8, 27, 42, 43
	25, 40, 59, 62, 64	37, 39, 49, 54, 65	34, 38, 41, 46, 63	36, 47, 55, 56, 60	48, 50, 51, 57, 61	45, 52, 53, 58, 66

$$a^{x\,(\min.)} = Np + 1$$

x=66, a= 2, 7,11,12,13,18,20,28,31,32,34,41,44,46,48,50,51,57,61,63 **(rac. pr.)**
x=33, a= 4, 6,10,16,17,19,21,23,26,33,35,36,39,47,49,54,55,56,60,65
x=22, a= 3, 5, 8,27,42,43,45,52,53,58
x=11, a= 9,14,24,25,40,59,62,64
x= 6, a=15,22,30,38
x= 3, a=29,37
x= 2, a=66
x= 1, a= 1

$p = 71$

$$a^2 = Np + r$$

$r =$	1,	2,	3,	4,	5,	6,	8,	9,	10,	12,	15,	16,	18,	19,	20,	24,	25,	27
$a =$	1	12	28	2	17	19	24	3	9	15	21	4	35	27	34	33	5	13
	70	59	43	69	54	52	47	68	62	56	50	67	36	44	37	38	66	58
$r =$	29,	30,	32,	36,	37,	38,	40,	43,	45,	48,	49,	50,	54,	57,	58,	60,	64	
$a =$	10	32	23	6	26	31	18	16	20	30	7	11	14	25	22	29	8	
	61	39	48	65	45	40	53	55	51	41	64	60	57	46	49	42	63	

$$a^5 = Np + r$$

$r =$	1,	20,	23,	26,	30,	32,	34,	37,	39,	41,	45,	48,	51,	70
$a =$	1,5,25	27,36,38	11,26,55	22,39,47	3,4,15,	2,10,37	13,31,41	6,8,30	21,28,34	42,41,56	18,19,24	9,12,16	7,23,33	14,17,46
	54, 57	48, 64	59, 62	52, 53	20, 29	43, 50	63, 65	40, 58	61, 69	67, 68	32, 49	45, 60	35, 44	66, 70

$$a^7 = Np + r$$

$r =$	1,	5,	14,	17,	25,	46,	54,	57,	66,	70
$a =$	1,20,30,32	10,15,16,24	7,11,31,46	14,21,22,33	5,8,12,18	28,42,44,53	4,6,9,38	2,3,19,25	13,17,35,47	23,26,34,39
	37,45,48	36,54,58	52,68,69	62,65,67	27,29,43	69,63,66	49,50,57	40,60,64	55,56,61	41,51,70

$$a^{x\,(\min.)} = Np + 1$$

x=70, a= 7,11,13,21,22,28,31,33,35,42,44,47,52,53,55,56,59,61,62,63,65,67,68,69 **(rac. pr.)**
x=35, a= 2, 3, 4, 6, 8, 9,10,12,15,16,18,19,24,27,29,36,38,40,43,49,50,58,60,64
x=14, a=23,26,34,39,41,51
x=10, a=14,17,46,66
x= 7, a=20,30,32,37,45,48
x= 5, a= 5,25,54,57
x= 2, a=70
x= 1, a= 1

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 73$

$$a^2 = Np + r$$

$a =$ 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, 27, 32, 35, 36, 37, 38, 41, 46, 48, 49

$r =$ {1 32 21 2 15 9 3 31 4 23 26 13 30 5 10 18 20 6 16 29 25 22 11 7 / 72 41 52 71 58 64 70 42 69 50 47 60 43 68 63 55 53 67 57 44 48 51 62 66}

$r =$ 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72

$a =$ {14 28 36 35 34 8 24 33 19 17 12 27 / 59 45 37 38 39 65 49 40 54 56 61 46}

$$a^3 = Np + r$$

$r =$ 1, 3, 7, 8, 9, 10, 17, 21, 22, 24, 27, 30

$a =$ {1, 8 25, 54 13, 29 2, 16 36, 41 43, 51 11, 15 33, 45 17, 63 35, 50 3, 24 34, 53 / 64 67 31 55 69 52 47 68 66 61 46 59}

$r =$ 43, 46, 49, 51, 52, 56, 63, 64, 65, 66, 70, 72

$a =$ {14, 20 27, 49 12, 23 7, 10 5, 28 26, 58 21, 22 4, 32 18, 57 42, 44 6, 19 9, 65 / 39 70 38 56 40 62 30 37 71 60 48 72}

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 72$, $a =$ 5,11,13,14,15,20,26,28,29,31,33,34,39,40,42,44,45,47,53,58,59,60,62, 68 **(rac. pr.)**

$x = 36$, $a =$ 6,12,19,23,25,35,38,48,50,54,61,67

$x = 24$, $a =$ 7,17,21,30,43,52,56,66

$x = 18$, $a =$ 18,36,41,57,69,71

$x = 12$, $a =$ 3,24,49,70

$x = 9$, $a =$ 2, 4,16,32,37,55

$x = 8$, $a =$ 10,22,51,63

$x = 6$, $a =$ 9,65

$x = 4$, $a =$ 27,46

$x = 3$, $a =$ 8,64

$x = 2$, $a =$ 72

$x = 1$, $a =$ 1

$p = 79$

$$a^2 = Np + r$$

$r =$ 1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 18, 19, 20, 21, 22, 23, 25, 26, 31, 32, 36

$a =$ {1 9 2 20 18 3 22 13 31 4 27 16 39 10 38 24 5 37 30 36 6 / 78 70 77 59 61 76 57 66 48 75 52 63 40 69 41 55 74 42 49 43 73}

$r =$ 38, 40, 42, 44, 45, 46, 49, 50, 51, 52, 55, 62, 64, 65, 67, 72, 73, 76

$a =$ {14 35 11 26 19 21 7 34 29 17 23 33 8 12 15 25 28 32 / 6 44 68 53 60 58 72 45 50 62 56 46 71 67 64 54 51 47}

$$a^3 = Np + r$$

$r =$ 1, 8, 10, 12, 14, 15, 17, 18, 21, 22, 27, 33, 38

$a =$ {1, 23 2, 31 40, 51 27, 63 37, 60 17, 66 47, 54 9, 21 20, 65 44, 50 3, 7 41, 43 8, 26 / 55 46 67 68 61 75 57 49 73 64 69 74 45}

$r =$ 41, 46, 52, 57, 58, 61, 62, 64, 65, 67, 69, 71, 78

$a =$ {34, 53 5, 36 10, 72 15, 29 6, 14 30, 58 22, 25 4, 13 18, 19 11, 16 12, 28 33, 48 24, 56 / 71 38 76 35 59 70 32 62 42 52 39 77 78}

$$a^{13} = Np + r$$

$r =$ 1, 23, 24, 55, 56, 78

$a =$ {1, 8,10,18,21,22,38 4, 5, 9,11,19,23,26 3,24,28,30,34,35,37 2,13,16,20,25,36,42 6,7,29,39,47,48,53 12,14,15,17,27,33,41 / 46, 52, 62, 64,65, 67 31,32,40,50,72,73 43, 54, 59, 63,66,77 44, 45, 49, 51, 55,76 56, 60,68,70,74,75 57,58, 61, 69, 71, 78}

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 78$, $a =$ 3, 6, 7,28,29,30,34,35,37,39,43,47,48,53,54,59,60,63,66,68, 70,74,75,77 **(rac. pr.)**

$x = 39$, $a =$ 2, 4, 5, 9,11,13,16,19,20,25,26,31,32,36,40,42,44,45,49,50, 51,72,73,76

$x = 26$, $a =$ 12,14,15,17,27,33,41,57,58,61,69,71

$x = 13$, $a =$ 8,10,18,21,22,38,46,52,62,64,65,67

$x = 6$, $a =$ 24,56

$x = 3$, $a =$ 23,55

$x = 2$, $a =$ 78

$x = 1$, $a =$ 1

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 83$

$$a^2 = Np + r$$

$r =$	1	3	4	7	9	10	11	12	16	17	21	23	25	26	27	28	29	30	31	33	36
$a =$	1	13	2	16	3	33	29	26	4	10	41	40	5	21	39	32	19	14	23	38	6
	82	70	81	67	80	50	54	57	79	73	42	43	78	62	44	51	64	69	60	45	77

$r =$	37	38	40	41	44	48	49	51	59	61	63	64	65	68	69	70	75	77	78	81
$a =$	28	11	17	37	25	31	7	36	15	12	35	8	27	20	22	39	18	34	24	9
	55	72	66	46	58	52	76	47	68	71	48	75	56	63	61	53	65	49	59	74

$$a^{41} = Np + r$$

$r =$	1	82
$a =$	1, 3, 4, 7, 9, 10, 11, 12, 16, 17, 21, 23, 25, 26, 27, 28, 29, 30, 31, 33, 36, 37	2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50
	38, 40, 41, 44, 48, 49, 51, 59, 61, 63, 64, 65, 68, 69, 70, 75, 77, 78, 81	52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80, 82

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 82$, $a = 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53,$
$54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80$ **(rac. pr.)**

$x = 41$, $a = 3, 4, 7, 9, 10, 11, 12, 16, 17, 21, 23, 25, 26, 27, 28, 29, 30, 31, 33, 36, 37, 38, 40, 41,$
$44, 48, 49, 51, 59, 61, 63, 64, 65, 68, 69, 70, 75, 77, 78, 81$

$x = 2$, $a = 82$

$x = 1$, $a = 1$

$p = 89$

$$a^2 = Np + r$$

$r =$	1	2	4	5	8	9	10	11	16	17	18	20	21	22	25	32	34	36	39	40	42	44
$a =$	1	25	2	19	39	3	30	10	4	27	14	38	33	17	5	11	37	6	22	29	24	20
	88	64	87	70	50	86	59	79	85	62	75	51	56	72	84	78	52	83	67	60	65	69

$r =$	45	47	49	50	53	55	57	64	67	68	69	71	72	73	78	79	80	81	84	85	87	88
$a =$	32	15	7	36	26	12	18	8	44	35	43	31	28	42	16	41	13	9	23	21	40	34
	57	74	82	53	63	77	71	81	45	54	46	58	61	47	73	48	76	80	66	68	49	55

$$a^{11} = Np + r$$

1,	12,	34,	37,	52,	55,	77,	88,
$a =$ 1, 2, 4, 8	19, 27, 29, 37	9, 18, 21, 36	3, 6, 7, 12	33, 41, 43, 61	5, 10, 17, 20	13, 15, 26, 30	11, 22, 25, 44
16, 32, 39, 45	38, 54, 58, 59	42, 49, 55, 69	14, 23, 24, 28	65, 66, 75, 77	34, 40, 47, 53	31, 35, 51, 52	50, 57, 73, 81
64, 67, 78	63, 74, 76	72, 79, 84	46, 48, 56	82, 83, 86	68, 71, 80	60, 62, 70	85, 87, 88

$$a^{x\,(\text{min.})} = Np + 1$$

$x = 88$, $a = 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54,$
$56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86$ **(rac. pr.)**

$x = 44$, $a = 5, 9, 10, 17, 18, 20, 21, 36, 40, 42, 47, 49, 53, 68, 69, 71, 72, 79, 80, 84$

$x = 22$, $a = 11, 22, 25, 44, 50, 57, 73, 81, 85, 87$

$x = 11$, $a = 2, 4, 8, 16, 32, 39, 45, 64, 67, 78$

$x = 8$, $a = 12, 37, 52, 77$

$x = 4$, $a = 34, 55$

$x = 2$, $a = 88$

$x = 1$, $a = 1$

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 97$

$$a^2 = Np + r$$

$r=$	1	2	3	4	6	8	9	11	12	16	18	22	24	25	27	31	32	33	35	36	43	44	47	48
$a=$	1	14	10	2	43	28	3	37	20	4	42	33	11	5	30	15	41	18	36	6	25	23	12	40
	96	83	87	95	54	69	94	60	77	93	55	64	86	92	67	82	56	79	61	91	72	74	85	57

$r=$	49	50	53	54	61	62	64	65	66	70	72	73	75	79	81	85	86	88	89	91	93	94	95	96
$a=$	7	27	21	32	35	16	8	29	39	19	13	48	47	46	9	45	38	31	34	24	44	26	17	22
	90	70	76	65	62	81	89	68	58	78	84	49	50	51	88	52	59	66	63	73	53	71	80	75

$$a^3 = Np + r$$

$r=$	1,	8,	12,	18,	19,	20,	22,	27,	28,	30,	33,	34,	42,	45,	46,	47
$a=$	1, 35	2, 25	18, 31	44, 65	26, 34	55, 57	6, 16	3, 8	5, 14	10, 28	47, 54	30, 80	23, 29	46, 58	20, 21	33, 73
	61	70	48	85	37	82	75	86	78	59	93	84	45	90	56	88

$r=$	50,	51,	52,	55,	63,	64,	67,	69,	70,	75,	77,	78,	79,	85,	89,	96
$a=$	9, 24	41, 76	7, 39	52, 68	13, 17	4, 43	38, 69	19, 83	11, 89	22, 81	15, 40	60, 63	12, 32	49, 66	27, 72	36, 62
	64	77	51	74	67	50	87	92	94	91	42	71	53	79	95	96

$$a^{x\,(\min.)} = Np + 1$$

$x=96$, $a=$ 5, 7,10,13,14,15,17,21,23,26,29,37,38,39,40,41,56,57,58,59,60,68,71 74,76,80,82,83,84,87,90,92 (rac. pr.)

$x=48$, $a=$ 2, 3,11,25,31,32,44,48,49,53,65,66,72,86,94,95

$x=32$, $a=$19,20,28,30,34,42,45,46,51,52,55,63,67,69,77,78

$x=24$, $a=$ 4, 9,24,43,54,73,88,93

$x=16$, $a=$ 8,12,18,27,70,79,85,89

$x=12$, $a=$ 6,16,81,91

$x=$ 8, $a=$33,47,50,64

$x=$ 6, $a=$36,62

$x=$ 4, $a=$22,75

$x=$ 3, $a=$35,61

$x=$ 2, $a=$96

$x=$ 1, $a=$ 1

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

$p = 101$

$$a^3 = Np + r$$

$r =$	1,	4,	5,	6,	9,	13,	14,	16,	17,	19,	20,	21,	22,	23,	24,	25,	30
$a =$	1	2	45	39	3	35	32	4	44	25	11	18	27	15	23	5	38
	100	99	66	62	98	66	69	97	57	76	90	83	74	86	78	96	63
$r =$	31,	33,	36,	37,	43,	45,	47,	49,	52,	54,	56,	58,	64,	65,	68,	70,	71
$a =$	43	29	6	21	12	34	42	7	31	16	37	19	8	41	13	26	24
	58	72	95	80	89	67	59	94	70	85	64	82	93	60	88	75	77
$r =$	76,	77,	78,	79,	80,	81,	82,	84,	85,	87,	88,	92,	95,	96,	97,	100	
$a =$	50	28	49	33	22	9	48	36	40	17	47	30	14	46	20	10	
	51	73	52	68	79	92	53	65	61	84	54	71	87	55	81	91	

$$a^5 = Np + r$$

$r =$	1,	6,	10,	14,	17,	32,	36,	39,	41,	44
$a =$	1, 36, 84	22, 30, 70	10, 32, 41	4, 33, 43	13, 20, 23	2, 67, 72	25, 25, 54	26, 27, 40	3, 7, 50	8, 53, 66
	87, 95	85, 96	57, 62	45, 77	64, 82	73, 89	80, 92	46, 63	59, 83	86, 90
$r =$	57,	60,	62,	65,	69,	84,	87,	91,	95,	100
$a =$	11, 15, 35	18, 42, 51	38, 55, 61	9, 21, 47	12, 28, 29	19, 37, 78	24, 56, 58	39, 44, 60	5, 16, 31	6, 14, 17
	48, 93	94, 98	74, 75	49, 76	34, 99	81, 88	68, 97	69, 91	71, 79	65, 100

$$a^{x\,(\min.)} = Np + 1$$

$x=100$, $a=$ 2, 3, 7, 8,11,12,15,18,26,27,28,29,34,35,38,40,42,46,48,50,51,53, 55,59,61,63,66,67,72,73,74,75,83,86,89,90,93,94,98,99 **(rac. pr.)**

$x=$ 50, $a=$ 4, 9,13,20,21,22,23,30,33,43,45,47,49,64,70,76,77,82,85,96

$x=$ 25, $a=$ 5,16,19,24,25,31,37,52,54,56,58,68,71,78,79,80,81,88,92,97

$x=$ 20, $a=$32,39,41,44,57,60,62,69

$x=$ 10, $a=$ 6,14,17,65

$x=$ 5, $a=$36,84,87,95

$x=$ 4, $a=$10,91

$x=$ 2, $a=$100

$x=$ 1, $a=$ 1

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

Tableau des racines primitives

Rac. pr.	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	5	5	.	.	.	.	.	.	.	.	.	.	.	Nombres premiers auxquels appartiennent										
	.	7	.	7	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	11	.	.	.	11	11	11	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	13	.	.	.	13	13	.	.	.	13	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	17	.	17	17	17	.	.	17	17	17	.	17	.	.	.	.	.	.	.	.	.	.	.
	19	19	.	.	.	.	.	.	19	.	.	19	19	19	.	.	.	.	.	.	.	.	.	.
	.	.	.	23	.	23	.	.	23	23	.	.	23	23	.	23	.	23	23	23	.	.	.	.
	29	29	.	.	.	.	29	.	29	29	.	.	29	29	.	.	29	29	.	29	.	.	.	.
	.	31	.	.	.	.	.	.	.	31	31	31	.	.	.	31	.	.	.	31	31	.	31	.
	37	.	.	37	.	.	.	.	.	.	.	37	.	37	.	37	37	37	37	.	37	.	37	.
	.	.	.	.	41	41	.	.	.	41	41	41	.	41	.	41	.	41	.	.	41	.	41	.
	.	43	.	43	.	.	.	.	.	.	43	.	.	.	.	.	43	43	43	.	.	.	.	.
	.	.	.	47	.	.	.	.	47	47	.	47	.	47	.	.	.	47	47	.	47	47	.	.
	53	53	.	53	.	.	53	.	.	.	53	.	53	.	.	.	53	53	53	53	53	.	.	.
	59	.	.	.	59	.	59	.	59	59	.	59	59	.	.	.	59	.	.	.	.	59	59	.
	61	.	.	.	61	61	.	.	61	.	.	.	.	.	.	61	61	.	.	.	.	.	.	.
	67	.	.	.	.	67	.	.	.	67	67	67	.	.	.	.	67	.	67	.	.	.	.	.
	.	.	.	73	.	.	.	.	.	73	.	73	73	73	.	.	.	.	73	.	.	.	.	.
	.	79	.	.	79	79	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	83	.	.	83	83	.	83	.	.	.	.	83	83	83	.	.	83	83	83	.	83	.	83	.
	.	89	.	.	89	89	.	.	.	.	.	89	89	89	.	.	.	89	.	.	.	89	89	.
	.	.	.	97	.	97	.	.	97	.	.	97	97	97	.	97	.	.	.	97	.	97	.	.
	101	101	.	.	.	101	.	.	.	101	101	.	.	101	.	.	101	.	.	.	.	.	.	.

Rac. pr.	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
	53	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	59	.	59	59	59	.	.	.	.	.	.	.	Nombres premiers auxquels appartiennent											
	61	.	.	61	61	.	61	.	61	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	67	.	.	.	.	.	.	.	.	67	.	67	.	.	.	.	.	.	.	.	.	.	.	.	.
	.	.	73	.	.	.	.	73	73	73	.	73	.	.	.	.	.	73	.	.	.	.	.	.	.
	.	.	79	79	.	.	.	.	79	79	.	.	79	.	.	79	.	79	.	79	.	.	.	79	79
	.	83	83	83	83	83	83	83	.	83	.	83	.	.	89	83	83	.	.	.	83	83	83	83	.
	89	.	.	89	.	89	.	89	89	89	89	89	89	.	.	89	.	.	.	89	.	.	.	89	89
	.	.	.	.	.	97	97	97	97	97	.	.	.	.	.	.	.	97	.	.	97	.	.	97	.
	101	.	101	.	101	.	.	.	101	.	101	.	101	.	.	101	101	.	.	.	.	101	101	101	101

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM

des nombres premiers depuis 3 jusqu'à 101.

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
les racines primitives ci-dessus.																								
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
29	29	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	37	.	.	37	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
41	.	41	41	41	.	.	.	41	41	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
43	.	43	43	43	.	.	43	43	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
47	.	.	47	47	47	.	47	.	47	.	.	47	47	47	47	.	47	47	47	.	.	.	.	.
53	53	.	.	.	53	53	53	53	53	.	.	.	53	.	53	.	.	.	53	.	.	53	.	53
.	.	.	.	59	59	59	59	59	.	.	59	59	59	59	.	59	59	59	.	.	59	.	.	59
61	.	.	.	61	61	.	.	.	61	.	.	.	.	.	.	.	61	61	.	.	.	.	.	.
.	.	67	.	.	67	67	.	67	.	.	.	.	.	.	67	.	.	67	.	67	.	67	.	67
73	.	73	73	.	73	.	73	73	.	.	.	.	73	73	.	73	.	73	73	.	73	.	.	.
.	.	79	79	79	.	.	.	79	79	.	79	.	79	.	.	79	.	.	.	.	79	79	.	.
.	.	.	.	.	.	83	.	83	83	.	.	.	83	.	.	83	83	.	83	83	83	.	.	83
89	89	89	89	89	89	.	89	.	89	.	.	89	.	.	89	.	89	.	.	89	.	89	.	.
97	.	.	97	.	.	.	.	.	.	.	97	97	97	97	97	.	.	.	.	.	.	.	.	.
101	101	101	101	.	.	.	.	101	101	.	.	101	.	101	.	101	.	.	.	101	.	101	.	101

76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
les racines primitives ci-dessus.																								
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	79	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
83	.	.	83	83	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
89	.	.	.	.	.	89	89	.	.	89	.	.	.	.	.	.	.	.	.	.	.	.	.	.
97	.	.	.	97	.	97	97	97	.	.	97	.	.	97	.	97	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	101	.	.	101	.	.	101	101	.	.	101	101	.	.	.	101	101	.

Brought to you by | University of Iowa Libraries
Authenticated
Download Date | 5/24/15 1:16 PM