NT-Cryptography MAT4930 *7554*

Sample Prereq-A

Prof. JLF King 1Sep2015

This practice prereq is much longer than the actual prereq will be.

A1: *In complete English sentences, on your own sheets of paper, please write,* (double-spaced)*, the following definitions and proofs, Do* **not** *restate the problem.*

i *A number $\beta \in \mathbb{C}$ is* ***algebraic*** IFF $\cdots$.

ii *The* ***degree*** *of β is...* .

p1 The Chinese Remainder Theorem says ____

____

____

____

____ .

p2 Let $T_n := 18^n + 1$ for $n = 3, 5, 7, 9, 11, \ldots$. Prove that each such T_n is composite.

p3 Define a sequence $\vec{\mathbf{b}} = (b_0, b_1, b_2, \ldots)$ by $b_0 := 0$ and $b_1 := 3$ and

†: $$b_{n+2} := 7b_{n+1} - 10b_n\,, \quad \text{for } n = 0, 1, \ldots.$$

Use induction to prove, for all $k \in [0..\infty)$, that

‡: $$b_k = 5^k - 2^k\,.$$

Further. Given recurrence (†) and initial conditions, *explain* how you could have discovered/computed the numbers 5 and 2 in the (‡) formula.

Can you generalize to getting a (‡)-like formula when the recurrence is $\boxed{b_{n+2} := \mathbf{S}b_{n+1} - \mathbf{P}b_n}$, for arbitrary real-number coefficients $\mathbf{S}$ and $\mathbf{P}$?

A2: Math-Greek alphabet: Please write the **two** missing data of lowercase/uppercase/name. Eg:

"iota: ____ α: ____ B: ____ ." You fill in: ι I A *alpha* β *beta*.

Σ: ____ Δ: ____ Υ: ____

γ: ____ ω: ____ ζ: ____

lambda ____ nu ____ rho ____ xi ____

A3: Show no work. Please write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

a And $y=$ ____ is the smallest natnum with

$$y \equiv_{20} 1, \qquad y \equiv_{15} 11, \qquad y \equiv_{12} 5.$$

b $N := \varphi(100)=$ ____ . So $\varphi(N)=$ ____ .
EFT says that $3^{1621} \equiv_N$ ____ $\in [0..N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are ____ ____ .

c Euler $\varphi(121000) =$ ____ .
Express your answer as a product $p_1{}^{e_1} \cdot p_2{}^{e_2} \cdot \ldots$ of *primes* to posint powers, with $p_1 < p_2 < \ldots$.

d May lightning ↯ strike this table! (I.e, please fill in.)

n	r_n	q_n	s_n	t_n
0	100	**—**	**1**	**0**
1	23		**0**	**1**
2				
3				
4				
5				
6				

Thus $1 = [$ ____ $\cdot 100] + [$ ____ $\cdot 23]$.

e LBolt gives $G := \text{Gcd}(1533, 413)=$ ____ . And $1533S + 413T = G$, where $S=$ ____ & $T=$ ____ are integers.

f LBolt: $\text{Gcd}(70, 42)=$ ____ $\cdot 70 +$ ____ $\cdot 42$.
So (LBolt again) $G := \text{Gcd}(70, 42, 60)=$ ____ and ____ $\cdot 70 +$ ____ $\cdot 42 +$ ____ $\cdot 60 = G$.

g Note that $\text{Gcd}(15, 21, 35) = 1$. Find particular integers S, T, U so that $15S + 21T + 35U = 1$:
$S=$ ____ , $T=$ ____ , $U=$ ____ .
[*Hint:* $\text{Gcd}\big(\text{Gcd}(15, 21), 35\big) = 1$.]

h Mod K:=50, the recipr. $\langle \frac{1}{21} \rangle_K =$ ____ $\in[0..K)$.
[*Hint:* ↯] So $x=$ ____ $\in[0..K)$ solves $4 - 21x \equiv_K 1$.

i Consider the three congruences C1: $z \equiv_{21} 18$, C2: $z \equiv_{15} 3$, and C3: $z \equiv_{70} 53$. Let z_j be the *smallest natnum* [or *DNE*] satisfying (C1) $\overset{\text{All}}{\ldots}$ (Cj). Then

z_2= ________ ; z_3= ________ .

j Consider the four congruences C1: $z \equiv_8 1$, C2: $z \equiv_{18} 15$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 3$. Let z_j be the *smallest natnum* satisfying (C1) $\overset{\text{All}}{\ldots}$ (Cj). Then

z_2= ________ ; z_3= ________ ; z_4= ________ .

k If $5^K \bullet\!\| 1000$, then K= ________ .

l If $7^e \bullet\!\| [2007!]$, then e = ________ .

m Let $N := 9876!$ (factorial). Written in base-10, this N ends in ________ many zeros?

A4: Here are High-school and calculus problems. Show no work. *NOTE*: The **inverse-fnc** of g, often written as g^{-1}, is *different* from the **reciprocal fnc** $1/g$. E.g, suppose g is invertible with $g(-2) = 3$ and $g(3) = 8$: Then $g^{-1}(3) = -2$, yet $[1/g](3) \stackrel{\text{def}}{=\!=} 1/g(3) = 1/8$.

Please write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

n Line $y = Mx + B$ is orthogonal to $y = \frac{1}{5}x + 2$ and owns $(4, 10)$. So M= ________ and B= ________ .

o The solutions to $7x^2 = 2 - 5x$

are x = ________ .

p $\left[\sqrt{5}^{\sqrt{2}}\right]^{\sqrt{32}}$= ________ . $\log_{81}(27)$= ________ .

q If $\log_B(64) = 3$ then B= ________ .

r Repeating decimal $2.3\overline{841}$ equals $\frac{n}{d}$, where posints $n \perp d$ are n= ________ and d= ________ .

s Compute the sum of this geometric series: $\sum_{n=3}^{\infty} [-1]^n \cdot [3/5]^n$ = ________ .

t For natural number K, the sum

$\sum_{n=3}^{3+K} 4^n$ equals ________ .

u $\sum_{n=1}^{\infty} r^n = \frac{5}{8}$. So r= ________ or **DNE**.

[*Hint:* The sum starts with n at **one**, not zero.]

v Let $y = f(x) := \left[5 - \sqrt[7]{x}\right]/3$. Its inverse-function is $f^{-1}(y)$= ________ .

A5: More proofs.

a *Prove:* THM: *There are ∞ly many primes.*

Start with... PROOF: FTSOContradiction, suppose

$*$: $p_1 < p_2 < \cdots < p_k < \cdots < p_{L-1} < p_L$

is a list of **all** prime numbers. I will now produce a prime q which *differs* from every member of ($*$), as follows. (*Continue your proof from here.*)