بسمه تعالی

مفاهیم پیشرفته معماری کامپیوتر	**تمرین ۱**	**نیمسال دوم ۹۶-۹۵**
دانشکده کامپیوتر	**تاریخ تحویل: شنبه ۹۶/۲/۹**	**مدرس: دکتر بیات سرمدی**

نکات

- تمرینات را سر موعد به استاد درس تحویل دهید.
- در صورت درج تمارین در بیشتر از یک صفحه، کلیه صفحات باید شامل نام، شماره دانشجویی و شماره تمرین بوده و با منگنه به هم وصل شده باشند.
- از قرار دادن تمارین در کاور خودداری فرمایید.
- سوالات در اولین کلاس تمرین بعد از موعد تحویل حل خواهند شد.
- اشکالات خود را در کلاس حل تمرین و یا از طریق ایمیل مطرح کنید.

mosanaei@ce.sharif.edu
salarifard@ce.sharif.edu

موفق باشید.

---

۱. میدان $GF(2^5)$ و چندجمله‌ای معرف میدان $f(x) = x^5 + x^3 + 1$ را روی $GF(2)$ در نظر بگیرید. بررسی کنید که $G(z) = z^2 + z + 1$ یک چند جمله‌ای بخش ناپذیر بر روی $GF(2^5)$ است. سپس با استفاده از دو چند جمله‌ای فوق اعضای میدان $GF((2^5)^2) = GF(2^{10})$ را تشکیل دهید. (کافی است اعضای هر میدان را بر حسب زیر میدان مربوطه نمایش دهید، یعنی $GF(2^5)$ برحسب $GF(2)$ و $GF(2^{10})$ بر حسب $GF(2^5)$).

۲. با استفاده از الگوریتم wNAF که در ادامه معرفی شده است، عدد ۱۱۰۱۱۰۱۱۱۱۱۰۰۱ را به فرم NAF تبدیل کنید.(w=4)

Algoritm 1: Mod function

```
If (d mod 2^w ) ≥ 2^(w-1)
        Return (d mod 2^w ) - 2^w
Else
        Return (d mod 2^w )
```

Algoritm 2: w-NAF method

```
i = 0
while ( d > 0 ) do
        if (d mod 2) =1 then
                d_i = d Mod 2^w
                d = d - d_i
        else
                d_i = 0
        end if
d = d/2
i = i +1
return (d_(i-1), ... d_1, d_0)
```

بسمه تعالی

مفاهیم پیشرفته معماری کامپیوتر	**تمرین ۱**	**نیمسال دوم ۹۶-۹۵**
دانشکده کامپیوتر	**تاریخ تحویل: شنبه ۹۶/۲/۹**	**مدرس: دکتر بیات سرمدی**

۳. عدد موجود در سوال بالا را یکبار با روش NAF ارائه شده در کلاس و یکبار با روش w-NAF (در سوال ۲ قبلا انجام شده است) به فرم NAF تبدیل کنید و سپس تعداد عملیات مورد نیاز برای انجام عملیات توان رسانی به روش پنجره لغزان (طول پنجره =۳) را بر روی این دو فرم با هم مقایسه کنید.

۴. با استفاده از الگوریتم ارائه شده در کلاس و با فرض $f(x) = x^7 + x^3 + 1$ حاصل جذر عدد $x^6 + x^4 + x^3 + x + 1$ را حساب کنید.